Shocking exposé of the
Election Commission's failure to
assure the integrity of India's electronic voting system

Democracy at Risk!

Can we trust our Electronic Voting Machines?

GVL Narasimha Rao

Democracy at Risk!

Can we trust our Electronic Voting Machines?

GVL Narasimha Rao

Democracy at Risk!

Can we trust our Electronic Voting Machines?

Published in 2010 by

Citizens for Verifiability,
Transparency & Accountability
in Elections
B4/ 137, Safdarjung Enclave, New Delhi 110 029
vetabooks@gmail.com, democracyatrisk@gmail.com
Phone: 91 9873300800 (Sagar Baria)

Printed in India by:
Sharp Prints, G-5, Red Rose Building,
49-50 Nehru Place, New Delhi-110019
Email: raman@sharppr.net

Dedicated to the Citizens of India:

They deserve a fully transparent and verifiable electoral system

Contents

*Foreword by Shri **L.K. Advani***
*Message from Shri **N. Chandrababu Naidu***
*Message from Prof. **David L. Dill**, Stanford University*
Acknowledgments

	Introduction	1
1	The India EVM Story	7
2	The Big Lie	19
3	Questionable Decisions of Election Commission	31
4	Faulty Machines Cause Tampering Concerns	41
5	Electronic Fixers Demand Hefty Sums	57
6	The X Factor	65
7	Vote of No Confidence	83
8	Farce of Enquiry by Election Commission	97
9	Commission Blocks Ethical Hacking	111
10	Voting Machines Demystified	123
11	Software Isn't Safe…	133
12	…..Nor is Hardware	147
13	Weak Links in the Chain	159
14	Hacking EVMs, Hijacking the Mandate	173
15	Are Indian EVMs Constitutional?	179
16	Restore Transparency & Verifiability	187

Annexures

List of Annexures

1. 'Resolution on Electronic Voting,' Verified Voting Foundation 195
2. 'Use of Electronic Voting Machines Unconstitutional' – Judgment of Federal Constitutional Court of Germany (Press Release) 197
3. 'We Do Not Trust Machines' (Article in *Newsweek*) 203
4. 'How To Trust Electronic Voting' (Editorial in *New York Times*) 206
5. 'The Good News (Really) About Voting Machines' (Article in *New York Times*) 208
6. 'A Single Person could Swing an Election' (Article in *Washington Post*) 213
7. Election Petition of Congress candidate Alok Jena in Orissa High Court (Extracts) 215
8. Writ petition of Subramanian Swamy in Delhi High Court (Extracts) 221

Foreword

In many democracies of the world the issue of electronic voting machines has become a matter of wide-spread public discussion. In India we have been conducting our elections through this device for the last two Lok Sabha elections and also in various Assembly elections held recently. But as yet there has been little debate on how useful these machines have proved. So when the author of this book G.V.L. Narasimha Rao approached me and requested me to write its Foreword, I not only accepted his plea, but complimented him for his efforts to compile all the facts he could on the subject and initiate a debate. The title of the book is certainly provocative.

Electoral Reforms has been my favourite subject of study since the mid sixties. When I was elected to Rajya Sabha in 1970, I discussed the matter with Shri Vajpayee who was at that time a member of Lok Sabha. He agreed to raise the issue in the Lower House, and try to have a JPC set up to study the question. Those days the issue of defections, abuse of governmental power in polls and growing misuse of money power in elections were three evils causing concern to everyone concerned with the health of Indian democracy. It was at the initiative of Shri Vajpayee that in 1970 a Joint Parliamentary Committee for Electoral Reforms was set up. Both he as well as I served on this Committee. This Committee proved short lived because the Lok Sabha was dissolved in 1971.

After the 1971 general elections, Shri Vajpayee raised the issue once again and saw to it that a new JPC was constituted. This Committee which gave its report in 1972 made several important recommendations some of which were accepted. The initiative taken by Vajpayee did not end there. Since then, several other committees have been formed, all aimed at reforming the poll process. My party has been proactively cooperating with all such efforts - be it the Tarkunde Committee (1974) or the Dinesh Goswami Committee (1990) or the Indrajit Gupta Committee (1998). The NDA Government headed by Shri Vajpayee also took several initiatives. But I must admit that the phenomenal increase in the cost of elections and increasing corruption that is being witnessed is extremely worrisome.

I understand that some time next month the Election Commission proposes to convene a meeting of political parties to discuss various issues relating to poll reforms. I have had occasion to speak to the Chief Election Commissioner myself and draw his attention to the evil of 'paid news', a form of media corruption which has besmirched recent elections. I understand that this issue is going to be discussed at this meeting. I suggest that the question of EVM also be taken up.

I personally regard it significant that Germany, technologically, one of the most advanced countries of the world, has become so wary of EVMs as to ban their use altogether. Many states in USA have mandated that EVMs can be used only if they have a paper back-up. So manufacturers of electronic voting machines in USA have developed a technology referred to as Voter Verified Paper Audit Trail (VVPAT). Every voter who exercises his vote on the EVM gets a print out in a ballot box so that if there is any discrepancy in the machine either because of mal-functioning or because of mischief the paper ballots can be counted.

Today 32 out of 50 states in the USA have passed laws making these VVPAT voting machines compulsory. The U.S. Congress has pending before it a federal law similar to that of the State laws. I think the Election Commission would be strengthening democracy if it contemplates similar legislation by the Indian Parliament also.

January 26, 2010 **L.K. Advani**

Message

There is an on-going debate in the country on the efficacy of EVMs in recording of votes according to the wish of the voter concerned. A leading non-governmental organization, Jana Chaitanya Vedika has demonstrated before the press the vulnerability of these machines. Sri Omesh Saigal, a former Secretary to the Government of India, has also complained that it is "possible and plausible" to manipulate EVMs to obtain a perverse result.

The standard defence put forward by the Election Commission of India is that the EVMs are manufactured and supplied by the leading public sector undertakings and they were introduced after a series of field trials and expert checks. However, the facts do not support the confidence expressed by the Election Commission. The experts highlight several lacunae which give rise to doubts about the integrity of the EVMs.

Credibility is the essence of the election process, and one cannot ignore the fact that technologically advanced countries like Germany, Ireland, Netherlands and the U.S.A. are either banning or prescribing stringent conditions for the usage of EVMs for registering the public vote.

I feel that it is incumbent on the Election Commission of India to address the concerns of the public seriously and to take steps to ensure that EVMs are used in future only with adequate safeguards.

I wish to congratulate GVL Narasimha Rao, whom I have known for many years, for the immense effort he has put in to bring out this important book. It presents a very comprehensive analysis of all the issues concerning EVMs, backed up by facts and the views of Indian and international experts. I do hope that the book opens up the issue for a national debate, and that we may soon have a reformed voting system in which our citizens can repose confidence.

February 1, 2010 **(N. Chadrababu Naidu)**

Message

Prof. David L. Dill
Stanford University

An important function of elections is to establish the legitimacy of the elected officials in the eyes of the public. Skeptical, untrusting observers should be able to see that election results are accurate. It is not sufficient for election results to be accurate; the public must know that the results are accurate. Civil society is damaged if elections are not credible, even in the absence of demonstrable fraud.

In traditional elections, paper ballots contribute to election credibility because voters can ensure that their votes have been properly recorded (when they write them on the ballot), and poll workers and observers at the polling place can ensure that ballots are not changed, added or removed after being deposited in the ballot box.

In contrast, purely electronic voting machines do not allow voters to verify that their votes have been accurately recorded, and do not allow observers to witness that the ballots have not been tampered with. Electronic voting machines provide no evidence during or after the election to convince a skeptic that the election results are accurate.

It is not clear that this situation would be acceptable even if electronic voting machines could be guaranteed to be accurate and honest. But such assurances are well beyond the current state of computer technology. It is not practical to design fully error-free and reliable computing equipment. More importantly, it is not feasible to prevent malicious changes to the machines' hardware or software. Electronic voting machines are especially vulnerable to malicious changes by insiders such as designers, programmers, manufacturers, maintenance technicians, etc. Of course, these problems are magnified enormously when the design of the machines is held secret from independent reviewers.

With current technology, the only trustworthy voting technologies are those that allow individual voters to verify that their votes have been properly recorded on a paper ballot. In

the United States, most voting systems rely on paper ballots that are filled out directly by the voters, and counted either by hand or by machine. If the votes are counted by machine, it is necessary to audit the performance of the machines by choosing groups of ballots at random and counting them by hand.

In 2003 in the U.S., I authored the ``Resolution on Electronic Voting,'' which has been endorsed by thousands of computer professionals including many of the World's most respected computer scientists. It states: ``Computerized voting equipment is inherently subject to programming error, equipment malfunction, and malicious tampering.''

It is time to recognize the reality that there is no basis for public trust in paperless electronic voting equipment.

This book by Mr. Narasimha Rao on Indian electronic voting machines brings out the fact that Indian EVMs are subject to the same questions raised about electronic voting in other countries. I hope that it will spark a long-overdue public debate on these issues.

David L. Dill
Professor of Computer Science

February 3, 2010

Stanford University, Gates Bldg Rm 344
Stanford, CA 94305-9030
Office: (650) 725-3642, Fax: (650) 725-6949
dill@cs.stanford.edu

Acknowledgments

This book would not have been possible without all those who shared much information and insights over the seven months that it has taken me to complete the effort. I owe my heartfelt thanks to each one of them.

For editing the book and making many suggestions over several weeks on content, style and design, I would like to thank K. Balakrishnan, formerly Research Editor of the Times of India. It was his suggestion that led me to focus on marshalling compelling arguments based on factual reports, field based evidences, published materials, international experiences etc and helped me to turn out something far more substantial than what would otherwise have been an academic discourse. Balakrishnan and I had co-authored a book titled "Indian elections in the Nineties" a decade ago.

Hari Prasad, managing director of NetIndia Private Ltd. and a "hactivist" was the key source of technical information and insights presented in this book. I would like to thank Hari Prasad and his colleagues Arun Kumar K, Vasavya Y, PSV Prasad and Suresh K for their invaluable contribution.

There are two eminent political leaders who lent moral strength to this effort. My heartfelt thanks to Shri L. K. Advani for readily consenting to write the Foreword for the book. A politician of unmatched intellect, Shri L.K. Advani is receptive to ideas and has recently done a blog on the EVMs on his personal website highlighting his concerns. As the Chairman of the BJP parliamentary party, I sincerely hope that he would take up the issue in parliament.

I owe gratitude to Shri Chandrababu Naidu, who readily agreed to write a message for the book. As India's first laptop-toting techno savvy politician, he understands both the positives and negatives of information technology. With his famed networking skills, I am confident that Shri Naidu will bring about a political consensus to effect necessary safeguards in our voting system.

A lot of background material on the subject was furnished by V.V. Rao, petitioner in the public interest litigation filed in the Supreme Court. I owe him a big thank you. Thanks are also

due to Satya Dosapati based in New Jersey for networking with many leading international experts on the subject.

Some of my colleagues also deserve my thanks: Parimal Kumar Singh for compiling information on international experiences and Shalu George for filing, typing many annexures and other background materials and printing several drafts of the chapters for review.

My wife, Mydhili Rao and my two school going sons, Vishal and Vineel have supported me throughout the period of writing this book. Mydhili read through many of my earlier chapters, gave suggestions to make it readable and kept my motivation high. My sons put up with my long hours on our home computer which I barely allowed them to use during the period.

My thanks are due to you, readers, for taking time off to read this book. I hope that this book would make you sit up, think and act in the interest of protecting our wonderful democracy.

I shall be happy to receive any comments and suggestions at nrao@drsindia.org

Introduction

Eternal vigilance is the price of liberty.
Thomas Jefferson

Electronic voting machines (EVMs) were introduced on an experimental basis in a limited way in Indian elections in 1982, and they have been in universal use since the general elections of 2004, when paper ballots were phased out completely.

Is it possible therefore to say now, that the horror stories of the earlier era – of doctored electoral rolls, voter intimidation, booth capturing, et al – are a distant memory, and that we have entered a new and glorious age of clean, free and fair elections? Though the Election Commission of India would have us believe so, the ground reality is different and quite disturbing.

It is noteworthy that over this period EVMs came into use extensively in many countries around the world, particularly in the U.S. and Western Europe. But their experience has not been happy. Everywhere, the electronic voting systems have come to be criticized, by citizens' groups, IT experts, lawyers and academicians, for not meeting minimal standards of system integrity, transparency, verifiability and allowing for a fair recount in case of disputes.

A group of over a thousand international technical experts have subscribed to a "Resolution on Electronic Voting' that categorically asserts*:

> "Election integrity cannot be assured without openness and transparency. But an election without voter-verifiable ballots [physical proof of voting] cannot be open and transparent: The voter cannot know that the vote eventually reported is the same as the vote cast, nor can candidates or others gain confidence in the accuracy of the election by observing the voting and vote counting processes."
>
> "There is no reliable way to detect errors in recording votes or deliberate election rigging with these machines. Hence, *the results of any election conducted using these machines are open to question.*"
>
> *http://www.verifiedvotingfoundation.org*

The Federal Constitutional Court of Germany (equivalent to the Supreme Court in India) in a landmark judgment in March, 2009 held that *electronic voting is unconstitutional because the average citizen could not be expected to understand the exact steps involved in the recording and tallying of votes by the electronic voting machines.*† Following the Court's verdict, Germany has banned use of electronic voting machines.

Holland and Ireland too have abandoned EVMs and have gone back to paper ballots. And developed and technologically advanced countries in our region like Japan and Singapore have so far stuck to paper ballot voting, owing to their simplicity, verifiability and voter confidence in the system.

Today, reliability of Electronic Voting Machines and the integrity of electoral verdicts is a subject of intense political debate and media scrutiny across the world.

* *See Annexure 1*

† *See Annexure 2*

Excerpts from two recently published reports in reputed international publications, the Newsweek magazine and the New York Times, would give a flavour of the prevailing opinion.*

Newsweek

We Do Not Trust Machines; people reject electronic voting

by Evgeny Morozov, Published May 23, 2009

A backlash against e-voting (on electronic voting machines) is brewing all over the continent (Europe)...State and local governments across the United States, much like European governments, are getting increasingly impatient with e-voting. Voters would be justified in (asking for) dispensing with e-voting altogether. At the moment, there's very little to like about it.

The New York Times

Editorial

How to Trust Electronic Voting

Published: June 21, 2009

Electronic voting machines that do not produce a paper record of every vote cast cannot be trusted...In paperless electronic voting, voters mark their choices, and when the votes have all been cast, the machine spits out the results. There is no way to be sure that a glitch or intentional vote theft - by malicious software or computer hacking - did not change the outcome. Few issues matter as much as ensuring that election results can be trusted.

Thirty-two of the 50 states in the U.S. have passed legislation making it mandatory to have verifiable physical record of every single vote cast. Another six

* *See Annexures 3 & 4*

states are following the same safeguards, though it is not mandatory according to their statutes.

In a 2005 report titled *Building Confidence in U.S. Elections*, Jimmy Carter (former president of the United States) and James Baker III (former secretary of state), co-chairs of the bipartisan Commission on Federal Election Reform suggested that all electronic voting machines be equipped with a voter-verifiable paper audit trail for the following four reasons.

a) To increase citizens' confidence that their vote will be counted accurately

b) To allow for a recount

c) To provide a back up in cases of loss of votes due to malfunction

d) To test – through a random selection of machines – whether the paper result is the same as the electronic result

Independent experts are agreed that Indian EVMs meet none of the above criteria. And the concerns on these grounds are by no means theoretical or academic. There have been complaints galore at the ground level by ordinary voters, political parties across the spectrum, and candidates contending that they have been unfairly denied their share of the vote. The complaints, requests for information under Right to Information (RTI) Act, election petitions and legal challenges filed in various High Courts and the Supreme Court have all been systematically stonewalled by the Election Commission of India (ECI) which maintains the ludicrous refrain that Indian EVMs are unique and 'tamper-proof'.

The truth, however, is not merely that our EVMs, like any other in the world, are prone to tampering in any number of ways by external hackers, but that the more insidious and ever present danger which the EC refuses to acknowledge is 'insider fraud' - by any of the

thousands of 'authorised' personnel having access to the machines. These include the Indian developers and manufacturers of the machines, the vendors supplying the components including the foreign companies who have been assigned the security-sensitive job of fusing the software onto the microchips sourced from them, the local officials who have the custody of the machines before, during and after elections, the technicians assigned for maintenance, repair and testing of the machines, etc etc. Field reports documented in this book clearly indicate that there is room for strong suspicion of insider fraud.

In our system of representative democracy, elections provide the only occasion when the people directly exercise their sovereign power. Immediately thereafter this power is ceded to the elected representatives. If this sacred power is vitiated by a voting system of dubious integrity open to insidious fraud, it is evident that our democracy is seriously endangered.

There is insufficient appreciation among the lay public of the facts and issues about this matter that vitally concerns them - largely due to the mystique concerning anything technological, and to the implicit faith in a constitutional body such as the Election Commission. Sadly, the national media has been complacent in this regard. However, the local media has been full of detailed factual reports on these matters which unfortunately do not find national salience.

This book has been written with the objective of filling this information and awareness gap. It is hoped that the issues raised herein will become a matter of national debate, leading to initiation of steps towards a reformed and truly transparent, verifiable and accountable voting system.

This is the year in which the Election Commission of India is celebrating its Diamond Jubilee. The Indian

public has a vital interest in ensuring that the year ends in something substantial to celebrate by way of a reformed voting system and not merely a celebration of the passing of years.

1

The India EVM Story

Electronic voting machines, like all other machines, are prone to errors and malfunctioning. No machine ever made anywhere in the world is infallible. They can never be. For instance, the electronic voting system installed in India's parliament, the country's most powerful institution in the country, has failed on a number of occasions and the members of parliament have had difficulty in registering their votes on the system.

In the crucial confidence vote to decide the fate of the Manmohan Singh government in September 2008, the whole nation witnessed on live television how as many as 54 elected members of the lower house of parliament failed to register their votes electronically. Utter chaos and confusion prevailed and finally, these members of parliament were allowed to vote manually.

If the country's lawmakers, 543 in number, have difficulty in voting on an electronic system installed in India's parliament, isn't it commonsensical to ask if India's 714 million strong electorate – many of whom can

neither read nor write – have any difficulty voting on electronic voting machines? We tend to assume that the voting system is working fine because we have never delved into the subject deeply.

The reality is that the electronic voting machines used in Indian elections, which belong to the class of what are internationally known as Direct Recording Electronic (DRE) voting machines, have failed on a number of occasions and suffer from numerous deficiencies. I have cited in chapter 4 several examples of how the electronic voting machines have malfunctioned in a number of states and constituencies. There are several instances of ballots lost and machines 'misbehaving' on a large scale resulting in disruption of the polling process.

Machines Prone to Manipulations

Machines are also prone to manipulations. Indian electronic voting machines are no exception. *If the computers in the prime minister's office and the personal computer of no less than the national security adviser, M.K. Narayanan have been hacked, isn't it ludicrous to assume that electronic voting machines locked up in store rooms in districts and remote rural locations would remain secure and not fall prey to the miscreants?*

There are several instances that we have come across where machines have 'switched' votes between candidates and have even 'produced' votes that were never cast!! All the field reports cited in chapter 4 are incontrovertible accounts of real happenings in the 2009 parliamentary elections and in the assembly elections that followed the same year.

Not just that. There are several personal accounts of senior politicians who have been approached by electronic "fixers" demanding hefty sums to fix elections in their favour. One such report pegs the asking amount for fixing an election in an assembly constituency at

Rs. 5 crore*. Sounds like a staggering sum? Not so today. Given the scale of corruption in Indian politics, it doesn't sound huge at all.

"Insider" Fraud a Concern

Personal accounts from well placed sources and experts say that those demanding these vast sums are "insiders". Who are these insiders? Unlike in the traditional ballot system where only the election officials were the "insiders", electronic voting machine regime has spawned a long chain of insiders, all of whom are outside the ambit and control of the Election Commission of India, the constitutional body vested with the authority to conduct free and fair polls. There is every possibility that some of these "insiders" are involved in murky activities in fixing elections. This is not hallucination. The whole world-except us in India – is alive to the dangers of insider fraud in elections, mostly by insiders in the electronic voting machine industry.

Jimmy Carter, former president of the U.S. and James Baker III, former secretary of state, co-chairs of the Commission on Federal Election Reform, U.S. in their report titled, "Building Confidence in U.S. elections" said, *"There is no need to trust the insiders in the election industry anymore than in other industries, such as gambling, where sophisticated insider fraud has occurred despite extraordinary measures to prevent it."*

The most important among the "insiders" are the manufacturers of India's electronic voting machines namely, Bharat Electronics Limited (BEL) and Electronics Corporation of India Ltd. (ECIL). Both are wholly government owned central public sector undertakings under the administrative control of the government of India.

* *In the commonly used Indian numbering system, one lakh equals 1,00,000 and one crore is 100 lakh or 10 million.*

In implementing the electronic voting machine regime, BEL and ECIL have in turn engaged the services of many others including foreign companies manufacturing microcontrollers (commonly referred to as chips) and private players and outsourcing agencies (some of which allegedly having political connections) for carrying out checking and maintenance of electronic voting machines during elections. They all are a source of potential hazard.

Another group that has a major role in maintaining the integrity of the voting machines is district administration in whose custody the EVMs are stored throughout their life cycle. As the same voting machines are commonly used in the same district over several elections, there are concerns regarding the security of the voting machines often stored in a decentralised manner in several locations in a district.

"Secret" Software Revealed to Foreign Companies

Shockingly, the EVM manufacturers, namely BEL and ECIL have shared the "top secret" software programming code used in the electronic voting machines with foreign manufacturers (Microchip, U.S.A and Renesas, Japan) to have it fused (copied) onto the microprocessors. These chips are then delivered to BEL and ECIL through their local vendors as 'masked' microchips (in case of ECIL) or 'One Time Programmable-Read Only Memory (OTP-ROM)' microchips (in case of BEL).

As the microchips delivered to the manufacturers are 'masked' or 'OTP-ROM', when the microchips are delivered, *the EVM manufacturers have no facility to read back the contents in the microchips to establish whether the microchips supplied to them have the original software or not.* Manufacturers of EVMs, BEL and ECIL can only carry out functionality tests on the electronic voting machines to check whether they are working properly or not. They cannot detect if the microchips supplied to

them have malicious programming. To say the least, this is shocking.

If the microchips in the electronic voting machines contain malicious software (commonly referred to as Trojan), elections results can be manipulated easily. Malicious programming can remain dormant during normal testing processes, but get activated later at the time of elections. This would result in an election fraud that can neither be detected before elections nor proved after elections.

Curiously, BEL and ECIL could have done the 'fusing' of the software onto microcontrollers in their own premises in a secure manner. That being the case, why did they prefer to do this in a foreign country? At whose instance was this decision taken and what were the compelling reasons for taking the decision? Was the Election Commission responsible for taking this decision? If no, did it approve of the decision by the manufacturers? And, was it at least aware of it? Despite repeated queries, there are no answers forthcoming from the Election Commission to any of these questions.

"Black Box Testing" by the Expert Committee

According to the RTI replies given by the Election Commission, the software program (referred to as source code) in the EVMs is not available with it. The Expert Committee of the Election Commission headed by Prof. P.V. Indiresan, which approved the EVMs currently in use in elections, has done "Black Box testing". This means that the Committee did not examine and certify the software program in the EVMs. It is the software in the EVMs that drives all its functions. By apparently not examining the software and merely relying on functionality tests, the Expert Committee has left a gaping hole in the security of the EVMs. This is horrifying.

"Black-box" and "White-box" Testing

State certification procedures [in the US for electronic voting machines] rely on a procedure called the "Logic and Accuracy" (L&A) test. The L & A test is called a "black-box" test, whereas examining the source code is called "white-box" testing.

According to Arnold B. Urken, who founded Election Technology Laboratories, the first voting-machine testing lab, white-box testing - eyes-on examination of the source code - should be mandatory if certification is to mean anything. Urken told me that he refused to certify ES&S (then called AIS) because the company would not allow him to examine its source code.

Bev Harris, author of Black Box Voting

"Authorised" Private Players Have Access to EVMs

Prior to elections, all electronic voting machines are subject to 'first level checks' in the field. These checks are carried out by "authorised" technicians deputed by the manufacturing companies. During these checks, the technicians have unfettered access to the voting machines. Physical access to the machines increases the risk of tampering.

Questionable Decisions

There are several decisions taken by the Election Commission which are questionable. First, the Election Commission has used as many as 9.3 lakh old electronic voting machines in 2009 parliamentary elections, ignoring the recommendations of its own Expert Committee. Only 4.48 lakh voting machines (about one-third of all EVMs used) are new or upgraded machines and meet the specifications suggested by the Expert Committee.

Secondly, the choice of states for the use of new/upgraded electronic voting machines is bereft of any logic

and even smacks of bias. New/improved EVMs have relatively improved security features and were supplied just before elections unlike old EVMs which have remained in storage for years and hence are more vulnerable. For instance, new EVMs were not used in any of the states ruled by the ruling United Progressive Alliance (UPA) coalition at the Centre in 2009 parliamentary elections.

Thirdly, electronic voting machines owned by some state governments were used in 2009 Lok Sabha polls. Many states buy the same electronic voting machines from BEL and ECIL for their use in local body elections. Due to the shortage of electronic voting machines that the Election Commission had directly purchased from the manufacturers, the Commission had allowed chief electoral officers of states to use EVMs owned by the state governments in the 2009 parliamentary polls. How does it matter who owns them, you may be wondering? It does matter. The Election Commission knows nothing about the integrity of the voting machines that have remained under the control of state governments. It has no way to even check if they are free from any bugs.

An election petition filed in the Orissa High Court by some Congress party leaders had alleged that 80,000 EVMs procured by the state government were used to manipulate 2009 assembly and Lok Sabha elections in the state. Ghulam Nabi Azad, General Secretary of the Congress party in charge of Orissa and present union health minister told the media after his party's disastrous performance in the state in 2009 polls, "EVMs were manipulated during the poll which resulted in the defeat of many Congress candidates." (IANS, June 18, 2009)

EC is Clueless on Technology

None of the election commissioners (neither the present commissioners nor their predecessors) has a proper understanding of the EVM technology. The same

goes for the entire administrative set up of the Election Commission of India. The Commission has a strong line up of young, impressive and suave deputy election commissioners. But they too have neither a technical background nor an appreciation of the vulnerabilities of the electronic voting machines that the Commission uses in elections. This glaring limitation became apparent to me in the couple of meetings that I had attended in the Election Commission of India to discuss vulnerabilities of electronic voting machines.

Owing apparently to its lack of familiarity, the Election Commission had delegated a number of crucial functions regarding the conduct of elections – like manufacturing, checking and maintenance of EVMs – to the manufacturers and other agencies over which it has no administrative control.

Recognizing the Election Commission's limitation, a CPI (M) delegation led by Prakash Karat which met the Commission in early September, 2009 suggested, "The entire manufacturing process has to be done under the control of the Election Commission and for this an exclusive technical department needs to be established."

"Faith based" Elections

An average Indian voter does not understand how an electronic voting machine works in recording and tallying votes. Most political parties and candidates do not have much understanding of these voting machines or the election operations involving them. Many of them have deep suspicions about the voting machines, but have spoken always in hushed tones for being ridiculed for their lack of knowledge and ignorance.

The Election Commission says that it has a number of checks and balances in place and people should "trust" the electronic voting machines despite their gaping security holes; then "trust" the myriad players – domestic public and private sector companies and

foreign companies – engaged in manufacturing and checking these machines and "trust" the district and local officials that guard these machines at all times and handle them at the time of elections with their woefully inadequate understanding of the technology, its limitations and their potential to manipulate elections?

All this begs a simple question: are we running "faith based" elections that we should "trust" all these insiders and not question their actions shrouded in mystery? We cannot pride ourselves being a vibrant democracy if our election results are reduced to merely our faith in agencies involved in the conduct of elections.

This excessive reliance on "faith" and not on what can you see and verify is a consequence of the new electronic voting regime. In the days of paper ballots, voters and candidates could see every stage of the voting process in a transparent manner. You saw what you got. In case of any doubt, you had the opportunity of a recount of individual physical ballots. In the electronic voting machines, votes are recorded electronically and if the data is manipulated and the original mandate gets lost, you would not get an opportunity to establish that this has been done and, of course, no consequential remedy is possible.

Viable Alternatives

How do we promote transparency in our voting system? If you want a simple solution, revert to the old paper ballot system. There is no system that can be more transparent than that. This is what a number of countries like Germany, Holland and Ireland have discovered after experimenting with the electronic voting machines. In Europe today, elections are predominantly conducted through paper ballots. That speaks a lot about a technology that was fashionable to adopt sometime ago but has been discarded for fear of undetected manipulation and lack of transparency.

If you firmly believe that India should not move away from electronic voting machines, which admittedly have some advantages, the next best thing is to adopt what is commonly referred to as Voter Verified Paper Audit Trail (VVPAT). Under VVPAT, the voting machines produce a paper record (a print out) of every single vote cast by the voters on the voting machines. After casting the vote on the EVM, the voter will examine the physical print out for its accuracy and if satisfied that there is no discrepancy, deposit the vote in a ballot box. This would ensure that even if the machine is manipulated, you still have the paper record to establish the election fraud.

VVPAT system generates a print out of every vote, much like the slip that the ATM machine spits out every time you carry out a transaction on it. Would you be comfortable with the idea of withdrawing or depositing cash in an ATM if it has no provision to give you a proof of transaction in the form of a print out? I am sure most people won't be comfortable with the idea. We all are very careful in protecting our money. Then, why do we become complacent and meekly surrender our sovereign right to choose our governments? Doesn't our democracy deserve better than these voting machines which function as black boxes and we as voters, have no clue as to what happens inside them?

In the United States, 32 of the 50 states have passed legislations mandating voter verified paper record and another six are maintaining physical record of every vote cast even without a formal legislation. There is a federal legislation pending in the U.S. Congress that seeks to mandate the paper record of every vote in the U.S federal elections. India needs a similar legislation. There is no reason why it would not work in India.

There is a writ petition filed in the Delhi High Court by Dr. Subramanian Swamy, former law minister seeking direction to the Election Commission to

introduce the VVPAT system in the electronic voting machines. The developments in the case will be keenly watched even as the Election Commission is resisting attempts to introduce transparency in the voting process.

Sordid State of Affairs in India

The Election Commission of India would have you believe that the electronic voting systems were banned in these countries because they were less secure than our indigenously developed electronic voting systems. No. They were banned not due to any evidence of electoral fraud but due to fears of tampering and lack of transparency associated with the electronic voting systems. If anything, these concerns and risks are much greater in India and thus warrant a serious scrutiny and study. This book is a serious research and investigative effort to expose the threats posed by the electronic voting machines to the sanctity of our electoral mandates.

Many of these countries where the electronic voting systems have been banned are mature democracies with more aware citizenry, a vigilant media and a proactive judiciary. On the other hand, India continues to persist with the electronic voting machines, despite their myriad problems. Lack of public awareness, lack of proper scrutiny by the media and a rather indifferent judiciary – courts have left all matters concerning electronic voting machines to the Election Commission of India which has a pre-judged mind on the issue – have all contributed to the sordid state of affairs in our country.

Raging Controversy

For the first time since their introduction in Indian elections, the EVMs have now become suspect in the eyes of the political class. A number of political parties have raised concerns regarding use of electronic voting

machines. A host of public interest litigations and election petitions have also been filed in the Supreme Court and High courts all across the country.

The raging debate on the reliability of the electronic voting machines in the aftermath of the 2009 parliamentary elections has brought to the fore several murky aspects regarding their development and use. Rather than address such concerns, the Election Commission of India has been making frenetic attempts to resist scrutiny and stifle criticism and concerns by spreading half truths about the electronic voting machines.

2

The Big Lie

If one lies, one should lie big.
Adolf Hitler

In his 1925 autobiography titled *Mein Kampf*, Adolf Hitler, the authoritarian German leader, referred to what he called the "Big Lie" technique. Hitler said:

> "A big lie always has a certain force of credibility; because the broad masses of a nation more readily fall victims to the big lie than the small lie. It would never come into their heads to fabricate colossal untruths, and they would not believe that others could have the impudence to distort the truth so infamously".

The Election Commission of India has applied the Big Lie technique to perfection to lay to rest serious concerns regarding EVMs in the wake of 2009 general elections. The Commission has done this by repeatedly saying that the "ECI-EVMs are fully tamper proof". Admittedly, this worked for the Election Commission as the vast masses of the country-media and elites included – as Hitler theorized, have fallen

victim to the colossal untruth fabricated by the Election Commission.

In a press statement dated August 1, 2009, the Commission said, "The Election Commission remains entirely satisfied that EVMs cannot be tampered with. These are fully tamper-proof." The three Election Commissioners, Navin Chawla, S.Y. Qureshi and V.S. Sampath have repeatedly stated that the "EVMs are fully tamper proof" at every opportunity.

That this is a "big lie" becomes clear from the 2006 Report of the Expert Committee set up by the Election Commission itself. The Report had categorically stated:

> "If the integrity of original program in the microchip is maintained, and the key pressed by the voter on ballot unit is faithfully recorded by the control unit, then the election through EVM will be fair." It adds, "The faithful recording of the voting data, unbiased & tamper proof functioning of control unit are critical to the conduct of a fair election."
>
> "....the Committee unanimously certifies that the EVM system is tamper-proof in the intended environment when due precautions are taken. For these reasons, the Committee recommends that the upgraded EVM with suggested modifications, testing and operating precautions may be accepted and put to use."

In other words, the Election Commission's Expert Committee had clearly said that tamper-proof working of the electronic voting machines could only be ensured if a number of conditions were met. Among them was the need to maintain the integrity of original program (source code) and use of upgraded EVMs with suggested modifications, testing and operating precautions.

In reply to an RTI query, the Election Commission has clearly stated that it does not check the originality

of the software installed in the electronic voting machines. Interestingly, the Election Commission maintains that it does not even have access to the EVM software. With these bare truths staring in the face, how on earth could the Election Commission guarantee the integrity or originality of the EVM software and ensure fairness of elections conducted through the electronic voting machines? Seen from that perspective, the Election Commission may be considered to have violated the constitutional mandate under Article 324 to hold free and fair elections.

The Election Commission had ignored another key recommendation of the Expert Committee; to use upgraded EVMs in elections. In the 2009 Lok Sabha election, the Election Commission had used as many as 9.3 Lakh 'old' EVMs (against only 4.48 Lakh upgraded EVMs). These old EVMs do not meet the security standards suggested by its own Technical Committee. Not just that; even after serious concerns were raised in the aftermath of 2009 general elections regarding the vulnerabilities of EVMs, the Election Commission had used old EVMs in the elections held to the states assemblies of Maharashtra, Haryana and Jharkhand in the second half of 2009.

Having failed to implement the most basic of requirements to maintain the integrity of Indian elections, the Election Commission's claim that its EVMs are "fully tamper proof" is absurd. It is evident that the Election Commission of India, a constitutional body, has resorted to falsification to mislead the public and the political parties that the ECI-EVMs are fail safe and fool proof.

All EVMs are "Tamper Prone"

A "Resolution on Electronic Voting" adopted by over a thousand technologists and academicians from United States of America says that all electronic voting systems can be deliberately corrupted at any stage and the

methods used are extremely difficult to foresee and detect. Here, we have the Indian Election Commission that assumes that nothing can go wrong with its electronic voting machines, whereas the whole world believes that the integrity of electronic voting systems cannot be taken for granted and adequate safeguards need to be provided.

> "All electronic systems are subject to subtle errors. Moreover, voting systems can be deliberately corrupted at any stage of their design, manufacture, and use. The methods used to do this can be extremely difficult to foresee and detect. Most importantly, there is no reliable way to detect errors in recording votes or deliberate election rigging with these machines. Hence, **the results of any election conducted using these machines are open to question.**"
> *http://www.verifiedvotingfoundation.org*

Burden of Proof on the Election Commission

David L. Dill, Professor of Computer Science and Electrical Engineering at Stanford University, an international expert on voting systems and a founder of the Verified Voting Foundation believes that the Indian Election Commission's repeated claims that its electronic voting machines are fully tamper-proof has no scientific basis. He believes that the burden of proof is on the Election Commission to show that it is difficult to commit an undetected election fraud using the Indian EVMs.

> ".....the legitimacy of elections depends on whether the populace can trust the results... the burden of proof should be on the advocates of an election system to show that it is difficult to commit undetected election fraud... No such claims should

be accepted unless the methods are disclosed and debated openly with experts on the other side." (Statement of Prof. David L. Dill of Stanford University in the Rejoinder Affidavit filed by Dr. Subramanian Swamy in the High Court of Delhi)

Our EVMs are "Different"

At a time when electronic voting machines across the world are being either discarded or subjected to stringent security and verifiability standards, the Election Commission is seeking to avoid any questions being raised on Indian EVMs by uttering untruth: that the Indian electronic voting machines are unique and different from the EVMs used elsewhere in the world and are infallible. A statement released by the Commission said:

"Not comparable with EVMs Abroad"

The Commission has come across some comparisons between ECI-EVM and EVMs used by foreign countries. Such comparisons are both misplaced and misguided. Most of the systems used in other countries are PC based and run on operating Systems. Hence, these could be vulnerable to hacking. The EVM in India on the other hand is a fully standalone machine without being part of any network and with no provision for any input. As already stated, the software in the EVM chip is one time programmable and is burnt into the chip at the time of manufacture. Nothing can be written on the chip after manufacture. Thus, the ECI-EVMs are fundamentally different from the voting machines and processes adopted in various foreign countries. Any surmise based on foreign studies or operating system based EVMs used elsewhere would be completely erroneous. The ECI-EVMs cannot be compared with those EVMs. (ECI Press Release, August 8, 2009)

Contrary to the Election Commission's contention, electronic voting machines used all over the world are "stand alone" machines. They are not part of any network, as inaccurately (and not inadvertently) suggested by the Election Commission. The effort needed to tamper with an EVM in India and elsewhere in Europe or the United States of America is nearly the same, irrespective of whether they run on operating system or otherwise.

The Election Commission's loud proclamations that the Indian EVMs are "different" are intended to mislead public opinion in the country and to escape public scrutiny at a time when the whole world is rejecting them and the very idea of "unverified" voting where machines only record votes electronically without any physical and verifiable record of voting.

Election Bodies Worldwide Resist Reform

If you are wondering why would a body like the Election Commission of India resort to such tactics, let me inform you that this is the nature and temperament of election bodies all over the world, not just in India. In no country in the world, election authorities took the initiative of reforming their voting systems and nowhere in the world have they taken kindly to any suggestions in this regard. It was only intervention of Courts, active role played by the civil society, the pressure exerted by the media and the legislative actions that have helped reform voting systems throughout the world.

Significantly, election authorities and vendors in countries like Germany, Holland, Ireland and the United States have all resorted to the application of the same "big lie" technique to ward off challenges to electronic voting machines in their countries. They all have claimed that their machines were not networked; they weren't computers but special purpose devices and therefore not prone to manipulation. But, in the end, their bluff was called and the voting machines were dispensed with.

Dr. Ulrich Wiesner, a physicist and software engineer who filed the lawsuit in the Federal

Constitutional Court of Germany finds that the Election Commission of India is adopting a similar approach as its counterparts elsewhere in the world. The Court had ruled in March, 2009 in the case filed by Wiesner that electronic voting was unconstitutional for lack of transparency and violation of the principle of democracy. I quote below a statement on Indian EVMs by Wiesner.

"(Electronic voting machines)..banned in the Netherlands, Irelands and Germany are not networked...similar to the Indian EVMs...work stand alone with no connection to internet or other networks during the election and counting phase. The lack of the network connection was one of the (invalid) reasons given by the vendor and by authorities in the three countries why the machines could not be hacked. The vendor also claimed that his devices were not real computers but special purpose devices which were designed to only count votes and could not be used for any other purpose....someone with access to the machines can replace the implemented software with any software, including vote stealing software.

"When the Indian Election Commission claims the (voting) machines are not riggable...it is common sense that someone who has sufficient access to open the machines and replace the software or hardware can implement virtually any functionality, including vote stealing functionality, that is only activated under certain circumstances and would not be spotted in tests."

(Statement of Dr. Ulrich Wiesner in the Rejoinder Affidavit filed by Dr. Subramanian Swamy in the High Court of Delhi in Writ Petition No. 11879 of 2009)

EVM is Secure as Software is "One time programmable"

"Software in the EVM chip is one time programmable and is burnt into the chip at the time of manufacture. Nothing can be written on the chip after manufacture," says the Election Commission. It is true that the software on the chip cannot be rewritten. But, ironically, the microchip that contains the software itself can be replaced with another tampered microchip and the EVM will continue to function normally. None of the checks presently conducted by the EVM manufacturers or by the technicians can detect any evidence of such tampering as the originality of the microchip in the EVM is not checked at any stage. Thus, no one can ever figure out if the original microchip is replaced with a fake one. That is how perhaps a number of hackers, referred to in chapter 5, are getting away with hacking EVMs.

'Authentication Unit' Project is Scrapped

The Election Commission gives the impression that checking the originality of software in EVMs is not possible as OTP-ROM or 'masked' chips are used. That is untrue. Not just the software, even the integrity of the hardware could be checked with the help of an authentication unit (or verification tool). The Expert Committee in its 2006 report had suggested that the manufacturers must undertake diagnostic checks and certify the integrity of both the hardware and the software of the EVMs. Accordingly, the upgraded EVMs developed by the manufacturers had provision for an interface to an 'Authentication Unit' which would have helped in detecting manipulation of EVM software & hardware. *However, shockingly, the Election Commission scrapped the project to develop and introduce the "Authentication Unit".* The details are as follows.

In 2006, the EVM manufacturers, BEL and ECIL engaged the services of SecureSpin, a software services firm in Bangalore for the development of the Authentication Unit. The authentication unit project

was discussed with the Expert Committee of the Election Commission and the prototype was readied by mid 2007 in accordance with the parameters spelt out by the Committee and tested with the EVM.

As the project was ready for implementation, mysteriously, the Expert Committee suddenly called it off. The General Manager (GM) of BEL under whose supervision the project was being implemented was transferred out. The new GM informed SecureSpin that the project had been shelved as per the directions of the Election Commission.

The prototype "Authentication Unit" that was mysteriously shelved.

By scrapping the project, the Election Commission has done away with a key component of the upgraded EVM system that was designed specifically to ensure the integrity of both the EVM software & hardware.

Tampering of EVMs being a serious concern, why did the Election Commission shelve the project? Repeated attempts to ascertain details in this regard did not yield any response from the Election Commission.

Complete Procedural Security is a Chimera

"The Commission has in place elaborate administrative measures and procedural checks and balances aimed at prevention of any possible misuse or procedural lapses," says a press release from the Election Commission dated August 8, 2009.

The Election Commission of India would like us to believe that these "checks and balances" are sufficient to prevent any mischief by any of all the thousands of "insiders" involved in election operations, including the

manufacturers, their suppliers and "authorised" technicians and local officials.

Just as in banks, there is a greater threat of electoral fraud from insiders than outsiders. This is the belief worldwide. "There is no reason to trust the insiders anymore in election industry than in any other industry," said Jimmy Carter (former president, U.S.) and James Baker III (former secretary of state, U.S.), co-chairs of the bipartisan U.S Commission on Federal Election Reform in a report titled *Building Confidence in U.S. Elections*.

"The concept that insiders will only tamper with certain things but not with electronic voting machines is ludicrous. And the concept that human nature will change if a machine is used, so that human beings will not tamper, is equally silly, "says Bev Harris, founder of Black Box Voting and an activist fighting for the voters' rights in the U.S.

EC Says We Don't Need Paper Back Up

All over the world today, transparency and verifiability of voting are the hallmarks of a credible voting process. Jimmy Carter and James A. Baker III stated in their report, "the purpose of voting technology is to record and tally all votes accurately and provide sufficient evidence to all participants – especially the losing candidates and their supporters that the election results accurately reflect the will of the voters."

Electronic voting machines that do not generate a voter verifiable physical record can neither give confidence to the voters that their vote had been properly recorded and counted nor can the candidates and parties get a fair opportunity of recount in cases of electoral disputes.

In its attempts to stifle opposition, the Election Commission of India has been defending the indefensible: a non-transparent and unverifiable voting

process. Today, the world finds paperless voting on Direct Recording Electronic (DRE) Voting machines unacceptable.

Prof. David L. Dill of Stanford University, USA and a strong votary of verified voting says:

> The right to have one's vote counted properly is a cornerstone of our democratic system. Making sure that our election systems are reliable and publicly verifiable enfranchises voters and increases public confidence and participation in our political process.
> *www.verifiedvoting.org*

In response to Dr. Subramanian Swamy's writ petition pending in the Delhi High Court seeking the Court's directions to the Election Commission not to use EVMs in elections unless they incorporate a (voter verified) paper trail of every vote cast, the Election Commission made the following statement in its counter affidavit:

> ".....if the system of paper trail is allowed to be used, the salient feature of the present system of being user friendly and simple to use and understand will be lost. Instead, the voter will be burdened to understand that he has not only to vote on the EVM but to obtain a ballot-receipt which he must then deposit in a ballot box. ...Even in present day and time, the system of elections is dependent on symbols only because of the uneducated and illiterate voter. How is he likely to read the ballot-paper printout? It is much possible that the voter will find such system as harassment and may even deter him from coming to the polling booth to cast the vote. Such system is likely to be counter productive."

The Election Commission's observations and apprehensions are unfounded. Commission's concern

that voters may perceive it as a burden is totally misplaced. Any step aimed at increasing the voter confidence and trust in voting will be welcomed by voters. That is how the whole world views it. If uneducated and illiterate voters could learn to vote on electronic voting machines, surely they would have no problem in reading the ballot-paper printout, which would also contain the same symbols?

With such unconvincing and irrational arguments, the Election Commission gives an inescapable impression that it has a vested interest in perpetuating the electronic voting system about which most parties today have serious concerns. A key question arises: why is the Election Commission so devoted to a voting system that is distrusted and discredited all over the world today? This will remain a subject of speculation as long as the Commission is seen to be blocking improvements and safeguards in electronic voting.

3

Questionabile Decisions of Election Commission

There are some major administrative decisions made by the Election Commission which show it in poor light. Two of these have turned out to be particularly consequential – the deployment of old model electronic voting machines in 2009 general elections, ignoring the recommendations of its Expert Committee, and the use of state government owned EVMs.

Use of Old EVMs

In the 2009 Lok Saba polls, as many as 13.78 lakh EVMs were deployed all over the country. Of these, only 4.48 lakh EVMs – less than one third – are new/ upgraded EVMs, which are as per the technical specifications prescribed by the Expert Committee report (2006) to make them "tamper-proof".

The remaining 9.3 lakh EVMs deployed are old EVMs which are less secure. The Election Commission's decision to ignore the recommendations its own Expert Committee that only the "upgraded EVM with suggested

modifications, testing and operating precautions may be accepted and put to use" raises serious questions. Why did the Election Commission, which had more than two years to act on the recommendations of the Committee, persist with the use of less secure EVMs in 2009 general elections? Not just that, why did the Election Commission use these old EVMs in the elections to the assemblies of Maharashtra, Haryana and Jharkhand, held after 2009 general elections?

Bias in Choice of States with New, Upgraded EVMs

Even more bizarre is the Election Commission's choice of states where the new, upgraded EVMs were used in 2009 Lok Sabha polls. The RTI reply cited above says that the Election Commission had deployed new EVMs in the states of Bihar, Chattisgarh, Goa, Gujarat, Uttar Pradesh, West Bengal, apart from all north eastern states except Assam. In all others states, old EVMs were used.

A look at the states where the new EVMs were used reveals that no meaningful criteria (like the geographic location of a state or its size or the phase in which the states went to polls) appear to have been used for the choice of states with new/ upgraded EVMs..

New/ upgraded EVMs were used in some states ruled by the BJP led National Democratic Alliance (Bihar, Chhattisgarh and Gujarat) and some ruled by major opposition parties (like the Left Front ruled West Bengal, Bahujan Samaj Party ruled Uttar Pradesh).

Significantly, the new/upgraded EVMs were not used in any of the prominent states ruled by the Congress party and its pre poll allies. Old EVMs were used in all states ruled by the Congress party or its allies, namely Andhra Pradesh, Assam, Delhi, Haryana, Maharashtra, Rajasthan and Tamil Nadu. (See Box on the opposite page)

In the alphabetical sequence in which states with

ELECTION COMMISSION OF INDIA

NIRVACHAN SADAN, ASHOKA ROAD, NEW DELHI-110001

No.RTI/2009-EMS/ 39 Dated: 21st July, 2009

Sh V. Venkateshwar Rao,
6-1-68/4/1 Second Floor, Lootheran Church Road,
Lakdikapool, Hyderabad-500004, Andhra Pradesh.

Subject: Information under RTI on EVMs

Sir,

I am directed to refer to your letter dated lst July, 2009 on the subject cited & to submit the information, as under:

I) About 13.78 Lakhs EVMs (the EVMs which are involved in Election Petitions/ Court cases were not used) were used in 2009 Parliamentary elections. Out of 13.78 lakh EVMs, 9.30 lakh EVMs were old machines and 4.48 lakh EVMs were new machines.

Old Machines:

Year	BEL	ECIL	Total
2000-01	66900	71274	138174
2001-02	72184	67754	139938
2002-03	94887	95697	190584
2003-04	167850	168195	336045
2004-05	38325	87286	125611
Total	**440146**	**4902061**	**930352**

New Machines:

Year	BEL	ECIL	Total
2006-07	137000	113000	250000
2008-09	106400	81600	188000
During LS'09	10000	0	10000
Total	**253400**	**194600**	**448000**

2) New machines mentioned above are upgraded EVMs as recommended by the Committee headed by Prof. Indiresan. **Upgraded EVMs were used in all the Parliamentary Constituencies of Arunachal Pradesh. Bihar. Chhattisgarh. Goa, Gujarat, Manipur, Mizoram, Meghalaya, Nagaland, Sikkim, Tripura, Uttar Pradesh, West Bengal, Andaman & Nicobar Islands, Dadra & Nagar Haveli, Daman & Diu and Lakshadweep.**

Yours faithfully,

(K. N. Bhar)
Under Secretary/CPIO

new/ upgraded EVMs are listed in the RTI reply, the UPA ruled states of Andhra Pradesh, Assam, Delhi, Haryana, Maharastra, Rajasthan and Tamil Nadu (which fall in the same sequence) are missing.

Was this a mere coincidence? On the face of it, it does not appear so. Who were the persons responsible for making these decisions? What was the basis for making such decisions? When were these decisions made? Persistent questions posed to the Election Commission by the petitioners in the Supreme Court, who were directed by the Supreme Court to approach the Election Commission, failed to elicit any response.

Old EVMs more Tamper-prone

Election Commission's later actions confirm that the old EVMs are more tamper-prone. In the by-elections held to Tamil Nadu assembly in August, three months after 2009 Lok Sabha polls, the Election Commission had used new/ upgraded EVMs following complaints of political parties that the EVMs used in general elections weren't reliable. If the old EVMs were indeed tamper proof, why did the Commission volunteer to use new, upgraded EVMs in by-elections?

On the other hand, if the old EVMs are indeed vulnerable, as the Commission seemed to acknowledge in Tamil Nadu by-elections, why did the Election Commission use the same old EVMs in the recent elections to the state assemblies of Haryana, Maharashtra and Jharkhand?

"Planned" Shortage of EVMs

Commissioning the required number of EVMs is necessary for the smooth conduct of elections. Election Commission failed to make a proper estimate of the required number of EVMs for the 2009 general elections. On October 1, 2008, six months before scheduled parliamentary elections in April-May 2009, the Chief Election Commissioner, N. Gopalaswami stated that the

Election Commission had estimated the requirement of EVMs to be 10.7 Lakh machines in 2009 general elections. (The Hindu, October 1, 2008)

To meet this requirement, the Election Commission had placed an order for supply of 1.8 Lakh new EVMs, of which 1.02 Lakh were sourced from the BEL and the rest from the ECIL. But, the actual number of electronic voting machines used in the 2009 parliamentary elections was 13.78 Lakh. Evidently, the Election Commission failed to properly estimate the EVM requirement for 2009 polls.

The above figures indicate that the Election Commission had under-assessed the EVM requirements in 2009 Lok Sabha polls by a whopping 3.08 Lakh machines. How it met the shortfall of electronic voting machines by such a large number is an interesting story.

State Government Owned EVMs

Throwing all caution to the wind, the Election Commission of India met the shortfall in the electronic voting machines by commissioning state government owned EVMs.

Some state governments buy electronic voting machines (EVMs) from the same manufacturers namely, BEL and ECIL to hold local body elections. Article 243 of the Constitution vests the responsibility of conducting elections to the Panchayats (and urban local bodies) in State Election Commissions, which are headed by State Election Commissioners appointed by the state governments.

The Election Commission of India has no superintendence powers over State Election Commissions as its mandate is confined to holding elections to only Parliament and legislature.

Days before the first phase of polling in 2009 general elections, the Election Commission had directed the

chief electoral officers of states (who work directly under the superintendence of the Election Commission of India) to paste "Election Commission of India" stickers on the state government owned EVMs used in parliamentary elections until the elections were over. Accordingly, the Election Commission of India had allowed use of state-owned EVMs in 2009 general elections. (EC letter no. No.51/8/7/2009-EMS dated 12th April, 2009) The letter is reproduced below:

ELECTION COMMISSION OF INDIA

Nirvachan Sadan, Ashoka Road, New Delhi-110001

No.51/8/7/2009-EMS Dated: 12th April, 2009

I am directed to state that some states are using the EVMs of State Election Commission of their states or of other states. It has been brought to the notice of the Commission that the EVM of State Election Commission are inscribed with the word 'SEC of Maharashtra' and so on. The day the ECIL arranged a demo of the SEC's 'Multi-vote' - 'Multi - post' EVM by setting for 'Single-vote' and 'Singlepost' a sticker was shown to the Commission like 'Election Commission of India'.

The Commission has decided that the states using the SEC's EVM will inform the manufacturer of the EVM to supply such sticker 'Election Commission of India' and paste it on the inscription of 'SEC of (name of the state)' on both the Control Units and Ballot Units. Once the election is over and such EVMs are being returned the sticker so pasted will be peeled off and the EVMs cleaned and then returned properly to the respective State Election Commissions.

Yours faith fully,

(K.N.BHAR)

While doing so, the Commission had either ignored or failed to realize that its decision to commission state government owned EVMs was fraught with serious security hazards. The integrity of voting machines that are owned by the state governments and have remained all along in the custody of some state governmental agencies is suspect. Details regarding the states and parliamentary constituencies where the state government owned electronic voting machines have been used are not available. That information could be quite revealing. The allegations by some Congress leaders in Orissa offer some insight.

Orissa Allegations

An election petition filed in the Orissa High Court by Alok Jena, Congress party's candidate in Bhubaneswar (Central) constituency made startling allegations.

In the election petition, the Congress candidate has alleged that the identification and machine numbers allotted to a number of polling stations have been changed and new EVMs were used in their place. In support of this claim, the petitioner has given details of all polling stations where such unannounced changes were made. (See Box on the next page)

The allegations in Orissa are indeed serious. The Orissa case signals the risks associated with the Election Commission's serious indiscretion in allowing the use of state government owned EVMs.

In respect of other states, it is not known as to how many state-owned EVMs were used in Lok Sabha elections. But, given the shortfall of over three lakh EVMs-the gap between what the Commission had purchased on its own and the number deployed in 2009 parliamentary elections – my guesstimate is that over three lakh state owned EVMs were used in 2009 general elections. Attempts to seek details in this regard have gone unanswered.

Election Petition of Congress Party Alleges Tampering

"According to the law and instructions of the Election Commission (of India), these EVMs were to be procured from recognized/authorized manufacturers / suppliers. In express violation of the above rule and instructions of the Election Commission, the agency in charge of conducting the state election for reasons best known to them procured 80,000 EVMs through *Idcol Software Limited*, which is a Government of Orissa undertaking and a group of hand picked, tainted officers were kept in its controlling and managing positions at the behest of Sri Pyarimohan Mohapatra during the relevant period on order to complete the process for EVM procurement. The trustworthiness of these EVMs was never tested nor demonstrated.

These EVMs were procured in two phases. In the first phase, 74,000 EVMs were procured but the same were not brought to the office of the chief electoral officer at Bhubaneswar nor to a place nearer to the office of the chief electoral officer at Bhubaneswar. On the contrary, it was directed to be stocked/ stored in the abandoned godown of Konark Jute mill at Dhanmandal. In the second phase, 6,000 EVMs were stocked and stored in unit-ix High school, Bhubaneswar"*

***

The Election Commission of India has endangered the security of electronic voting machines by deploying old EVMs and allowing the use of state government owned EVMs.

The next time around, if the Election Commission falls short of EVM requirements, don't be surprised if it allows use of EVMs owned by political parties or individual candidates!!

** See Annexure 7 for more details*

Or, it may allow private companies – some corporates had dialogue with EVM manufacturers to buy EVMs! – to deploy their EVMs to meet the shortfall.

In the field of electronics, frequent changes in technology and design warrant repeated replacement of old machines with new to keep them secure and up-to-date with technology. Let alone effecting such constant improvements, the Election Commission has failed even to ensure proper working of the EVMs as voters across the country, specifically in the states of Tamil Nadu and Orissa, have encountered serious problems on the polling day in voting on the EVMs raising serious questions about their integrity.

In a country where the 543 lawmakers elected by the nation's electorate to the lower house of Parliament cannot vote properly on an electronic voting system, it is hard to assume that its 714 million strong electorate – a third of whom can neither read nor write – has no problem voting on EVMs.

4

Faulty Voting Machines Cause Tampering Concerns

You won the elections, I won the count.
Anastasio Somoza

Have the electronic voting machines helped in maintaining the integrity of electoral verdicts, or are they largely responsible for the surprising and unexpected election outcomes in Indian elections? Do ordinary voters – many of whom lack even basic literacy skills – find voting on electronic voting machines easy and comfortable? These are some questions that merit a proper scrutiny.

On July 22, 2008, a crucial vote was held in India's lower house of Parliament, the Lok Sabha. The vote was to decide the fate of the Manmohan Singh led UPA government at the Centre which was reduced to a minority following the withdrawal of support to the government by the Left front.

In the parliament, there is a provision for members to vote on the electronic voting system fitted in their seats. All that the members were required to do was to press the button correctly to register their vote either in support or against the confidence motion moved by prime minister.

To everyone's shock, the votes of as many as 54 of the 543 elected Lok Sabha members were not registered on the electronic voting system. This is not an isolated incident. Similar scenes are witnessed every time the electronic voting system is used in parliament. Members do not press the buttons correctly and or the system does not record their votes properly; and a round of manual voting follows with a number of MPs being issued paper ballots.

sify news

Confusion after electronic voting shows govt win

IANS, 2008-07-22

New Delhi: There was considerable confusion in the Indian parliament Tuesday night, after a day of high drama, after results of electronic voting showed Prime Minister Manmohan Singh's government win the crucial confidence vote in the Lok Sabha by 253 votes to 232.

The voting recorded two abstentions in a house with 487 votes registered. Apparently, many members had either not voted properly or had waited to do manual voting that the Speaker said would follow. However, it was later announced that 54 votes were still to be counted, including of four members who voted in the inner lobby. They included former prime minister Atal Bihari Vajpayee who could not be present in the chamber because of illness.

Speaker Somnath Chatterjee said the final results were yet to be declared, but MPs began crowding around a smiling Prime Minister and Congress chief Sonia Gandhi to congratulate them.

In a country where the 543 lawmakers elected by the nation's electorate to the lower house of Parliament cannot vote properly on an electronic voting system, it is hard to assume that its 714 million strong electorate – a third of whom can neither read nor write – has no problem voting on EVMs.

Ordinary voters do have a problem voting on EVMs. It is just that no one looked into their problems with an open mind and presented them with alternatives. This chapter attempts to document many such problems.

Voters' Problems with EVMs

A news report filed by the news agency IANS in the November-December 2009 Jharkhand assembly elections caught my attention.

Nirmal Ho, a tribal and a marginal farmhand in the Chatarpur block of Palamau district, who feels that ballot papers were easy to understand, is more scared of the EVMs than of the Maoists who have been intimidating voters in the region. Stories like these make you wonder if the EVMs have truly served the interests of the country well. (See box)

EVM Failures

The EVM related problems cited in this chapter have been gathered from a plethora of sources and with limited resources and efforts. The magnitude of such problems in my assessment is quite large and this is borne out by reports in the local press and personal experiences of candidates contesting elections. However, the Election Commission which should be compiling such information and analysing it with a view to remedying the system refuses to acknowledge the problem and repeatedly claims that the electronic voting machines are "foolproof and fail safe," while there is a whole lot of evidence to the contrary.

Tribal voters in Jharkhand reckon with EVM technology

Published: Fri, 20 Nov 2009 at 10:04 IST

Fifty-year-old Hasulal Topno has never seen an electronic voting machine (EVM)

The impoverished Oraon tribal, who gathers firewood from the forest outlying the Palamau Tiger Reserve, a Maoist hotbed 35 km from Daltonganj town, got his voter identity card two years ago. "This is the first time I will vote in my life and I am so excited," the malnourished tribal, a father of four, told IANS. "But I am scared of the voting machine. I heard from the villagers that people have to cast their votes in a machine. I am illiterate, so is my wife as well as my eldest son who is 19. We will all vote this year."

Nirmal Ho, a tribal and a marginal farmhand in the Chatarpur block of Palamau district, is *more scared of the EVM than of the Maoists*, who have clamped down an unwritten election boycott whip. "Technology scares me. I have never been to school; neither have my forefathers," the elderly man told IANS. Ho will take a day off to attend an EVM demonstration in Chatarpur town December 6.

EVMs are still not a familiar sight in tribal Jharkhand, barring the urban pockets, because of inaccessibility, Maoist violence, illiteracy and poor awareness. "Our women are scared of such complicated machines. The ballot papers were easy to understand. Earlier, someone would point out the symbols and we would vote," the head of the group, Subal Mahto, told IANS. (Source: IANS)

Machine Problems frustrate voters

The Case of Tamil Nadu

In hundreds of polling stations across Tamil Nadu, voting machines frustrated voters, leading to disruption in voting and replacement of voting machines midway during polling. In many polling stations, complaints by voters were ignored and the polling was held even when

the problem persisted. The case of Tamil Nadu in 2009 general elections perhaps qualifies as one of the worst ever elections conducted using electronic voting machines.

Different types of problems were cited by voters all across Tamil Nadu. The most common problems are as follows:

- *When the voters pressed the button to vote for one party, the light flashed on another:* At several places, AIADMK supporters complained that the light flashed against the DMK symbol when they pressed the AIADMK button. Perambalur parliamentary constituency (Manachanallur), Villupuram P.C (Keezhappalayam, Namachivapuram, Melur, Thagamtheerthapuram, Karunguzhi), Coimbatore P.C (polling station nos. 49 in the city, 13 and 14 in Singanallur assembly), Pollachi P.C (polling station no. 107)
- *Light did not flash after vote was 'cast' in the EVM:* Perambalur P.C (Veppanthattai), Thanjavur P.C (Booth No.162 in Mannargudi assembly)
- *EVM did not produce beep sound raising suspicions:* Mayiladuthurai P.C (Tandamthottam, Tirunarayur)
- *Buttons got stuck and did not function:* Mayiladuthurai P.C (Vilandakandam Panchayat, Cholanmaligai) Papanasam P.C (Ayyampetai, Ammapetai), Thanjavur (Senthalai, Nagathi)
- *EVM gave continuous non stop beep:* Kumbakonam P.C (Tirunallur)
- *The voting machine did not make beep sound after casting the vote:* Mayiladuthurai P.C (Darasuram, Kumbakonam polling station no. 99, Papanasam P.C (Keelakovil-158, Vilayapetai-179, Tiruvalanchuli-180, Sundaraperumalkovil-183), Coimbatore P.C (Coim-batore North assembly-polling station nos. 43, 47)
- *Multiple beeps were produced by the EVMs, but ignored by officials:* Coimbatore P.C (Singanallur assembly–

polling station nos. 38, 165, 52, 150, 2, 13, 29, Coimbatore North assembly-polling station nos. 3,1) and Pollachi P.C (PS No. 92)

- *Seals found broken:* in Trichy West Assembly Constituency, Ward No. 51, polling station 66A, two paper seals (Nos. 15AA017514 & 15AA017515 were found to be damaged.

The Case of Orissa

In Orissa, which went to Lok Sabha polls on April 16 and 22, 2009 voting was delayed in a number of polling stations across the state due to faulty EVMs. The Congress and BJP supporters alleged that the EVMs did not record votes in favour of Congress and BJP candidates and irrespective of whichever candidate they chose, the votes were being recorded in favour of Biju Janata Dal (BJD) candidate only. Voters became agitated and clashed with polling officials at some places suspecting foul play.

A report in the popular website, *Orissa Matters* published on April 20, 2009 vividly captures the situation. Opposition parties including the Congress and the BJP and many common voters in Orissa felt that the electronic voting machines have been tampered with in the state. (See box)

In Maharashtra, votes given to any candidate in booth no. 265 of Mukhed Vidhansabha in the Nanded Parliamentary Constituency in Maharashtra were being recorded in favour of the Congress. A similar problem was noticed in booth no. 183 of Shivadi Assembly in the South Mumbai Parliamentary Constituency.

Another major problem cited by voters across the country is that the polling officials suspend voting for some time saying that the EVM has developed some problem. The polling is resumed shortly thereafter after "setting" the machine in order raising suspicion in the minds of the voters that officials may be up to some mischief. There seems to be

some basis for such suspicion as the polling officials know nothing more than operating the machine. How could they be repairing them?

Electronic voting machines tampered with in Orissa?
Posted on April 23, 2009 by Subhas Chandra Pattanayak

Subhas Chandra Pattanayak

Second and final phase of voting in Orissa is witnessing voters' wrath against polling officers in most of the booths as till now, i.e. noon, the Electronic Voting Machines (EVM) are not working. In the first phase of election on April 16, EVM problems had affected voting in many booths. Voters had taken that to be technical defects. Many voters had gone back from the booths and the day's last information from the Chief Election Officer had put the polling percentage at 52.6%. But on April 17, the percentage was finally placed at 65.9%. This enhancement was attributed to casting of votes beyond the voting time as that was allowed to compensate time lost due to defect in EVMs. This high rise in voting numbers was looked at askance in certain quarters, even though general public had accepted it as normal.

But the present scenario is so massive that many people suspect that the EVMs are tampered with. The EVMs are high-tech machines created with excellent technical know-how and carry certificate of faultlessness on the basis of meticulous testing. They should not have shown such defects in normal condition; but they may develop defect only if tampered with, suggest techno-academics that we contacted.

No wonder, voters in a Cuttack booth have manhandled the polling staff suspecting tampering of the EVMs. Apolitical intellectuals feel that there should be credible inquiry over non-functioning of the EVMs in such massive scale.

http://orissamatters.com/2009/04/23/1389_evm/

As all the EVMs are checked and certified by the "authorised" technicians of the manufacturers barely a couple of weeks before their deployment in elections, what could be the reasons for the malfunctioning of EVMs on a large scale? The only plausible reason is their manipulation and tampering. This disproves the Election Commission's claims that the EVMs are fail safe and tamper proof.

Lost Ballots

Vote is a sacred right enjoyed by citizens in a democracy. Nothing should prevent a voter from exercising this right. The EVMs have usurped this basic human right of voters at many places as their votes went missing either due to technical glitches or tampering of EVMs.

At many polling stations, EVMs worked perfectly on the polling day, but failed to read the stored voting data on the counting day. We have come across a large number of such cases in which the EVMs failed to read data stored in the memory of the EVMs. In all such cases, the returning officers discarded the polling data.

For instance, in Andhra Pradesh, in six polling stations of Parkal assembly constituency (numbering 185, 197, 209, 212, 221 and 224), all the votes cast in the control units have been lost. A similar situation was observed in several other constituencies: Ramagundam assembly constituency (polling stations 60 and 61), Alampur (SC) constituency (polling stations 60 and 69), Panyam (polling stations 44 and 45). This is only an indicative list and not exhaustive.

In Puducherry parliamentary constituency, in polling station no. 6 of Ozhukarai assembly segment, all the 555 votes were discarded as the control unit malfunctioned on the day of counting.

In a number of cases, where the control units (of EVMs) were replaced midway on the polling day due to

malfunctioning of EVMs, the votes polled in the faulty EVMs could not be retrieved.

To cite two such instances, in the assembly constituency of Pedakurapadu (Andhra Pradesh), in Nagireddypalem Village, the control unit was replaced in polling station number 2 as the EVM malfunctioned. 122 votes polled in the replaced EVM were discarded. In a similar incident, in Uravakonda assembly (A.P) 120 votes polled till the first EVM developed a problem were discarded.

In Tamil Nadu, a large number of voting machines were replaced due to their malfunctioning. In several such cases, the voting data stored in the malfunctioning EVMs was lost. In Tiruchirapalli city, in Ward number. 36 and Polling station no. 96, 289 votes were lost which were cast until 11.30 A.M in the morning when the voting machine was replaced. Similarly, in Coimbatore parliamentary constituency, votes were lost in the following polling stations: PS No. 38 (ward number 2), PS No. 149 (ward number 12), PS No. 25 (ward number 19), PS No. 34 (ward number 58), PS No. 55 (ward number 61).

The EVM is like a black box in which you cast your vote. You don't know what happens to it. It does not generate any physical record of voting. As a result, if the EVM fails to read the data stored in its memory, the voting data gets left out. Voters in such polling stations feel 'cheated' as their democratic choice finds no expression in the results.

A news report on elections in Finland reports that 2% of votes cast on electronic voting machines were lost leading to the Court's decision to cancel the election result. The irony in our case is that we don't even know the scale of such 'errors' and the extent of missing votes.

techdirt

On Second Thought, Finnish Gov't Rejects Defective E-Voting Results

Back in February, we found it disturbing that Finland was allowing the results of an election to stand, despite the fact that at least 2% of the votes had gone missing due to e-voting glitches. However, it looks like some sense of sanity has been restored as a higher court has now rejected the election results and ordered a new election. One hopes that the new election won't involve similarly screwed up e-voting machines. Speaking of which... in a separate article, we find yet another story of e-voting machines that were "mis-calibrated" in such a way that made it difficult to impossible for people to vote for candidates of their choice. At some point, given all of these problems with e-voting machines, you have to ask why elections officials still rely on them.

http://www.techdirt.com

EVMs Record More Votes than were Cast!

There are other instances of "discrepancies" in vote counts. On the polling day, after the polls close, the presiding officers hand over Form 17-C to the polling agents of all parties which contains the number of votes polled in that polling station. This number is sacrosanct and no votes can either go missing or get added to this after the polls close.

But in a large number of polling stations, differences have been observed between the number of votes actually polled on the polling day (as recorded in form 17-C) and the votes retrieved from that EVM on the counting day.

In Bhandara (Maharashtra) parliamentary constituency, difference was observed between the

votes polled and votes counted in respect of 61 polling stations.

In the elections held to Maharashtra assembly in October, 2009, similar discrepancies were reported. In one assembly constituency, the number of votes counted from the EVMs was more than the number of votes polled, while in another assembly, votes counted from the EVMs was less than the number of votes actually polled on the polling day. Both the cases reported in the Times of India raise suspicion.

THE TIMES OF INDIA

Tiroda, Arjuni-Morgaon EVMs under cloud

TNN 25 October 2009

GONDIA: The discrepancy in the actual figures of polling and shown by the electronic voting machines (EVMs) on the counting day has raised doubt in two assembly constituencies in Gondia district - Tiroda and Arjuni-Morgaon.

According to official figures of voting which were made available to the media on October 14, and the figures shown by EVMs did not tally. There were some discrepancies in the figures of voting on date of counting in Tiroda and Arjuni-Morgaon. The issue has gained importance as the difference in the top two candidates was 623 votes.

According to figures given on October 14 out of 1,97,696 voters 1,42,700 cast their franchise, whereas on the October 22, the EVM figure showed 1,43,056. The difference was of 356 votes. These votes could have made a lot of difference in final tally. However, as the difference of the votes between both candidates was over 500, recounting was rejected.

In Arjuni-Morgaon out of 2,02,556 voters, 1,49,061 exercised their franchise. However, after counting the total votes received by all contestants comes to 1,49,390. Here the difference is of 329 votes.

Perhaps, anticipating such problems, in a number of polling stations in Orissa, it was alleged that the mandatory Form 17-C was not even issued!

According to reports available, there are huge discrepancies between votes actually polled and votes counted in several polling stations across the country. These problems go unreported in the national media as the entire focus on the Election Day is on declaring the winners and the overall performance of leading parties.

In the present EVM regime, counting and declaration of results happens so fast that no one gets to notice anything. Once the result is out, nobody even bothers to know the details. The results of 2009 general election were practically known by 10 A.M, less than two hours after the counting began.

Machines "Switching" Votes

In Noida parliamentary constituency (Uttar Pradesh), independent candidates received 415 of the 417 votes polled in polling station located in Sector 25, Jalvayu Vihar. All the major political parties together received only two votes. The details are as under:

PC Name	- Gautambudh Nagar
AC Name	- Noida
Booth No.	- 61
Location Jalvayu Vihar, Sec.	- 25
Total Votes polled	- 417
Anil Kumar (Independent)	- 247
Sher Singh (Independent)	- 153
Rishi Singh (Independent)	- 9
Other Independents	- 6
Mahesh Sharma (BJP)	- 1
Samajwadi Party	- 1

We have contacted over 100 voters in the polling station area who categorically stated that they have

neither voted for any of these "independent" candidates nor have they even heard of them. Many voters recalled that the voting machine had malfunctioned for half an hour and this could have resulted in this fake outcome.

***

In Ghaziabad (Uttar Pradesh) parliamentary constituency, an independent candidate by name Satish secured only 998 votes in 24 rounds. But, all 501 votes polled in polling station No. 247 went to him and the candidates of the BJP and Congress received no votes at all and the BSP candidate Amar Pal Sharma got just 1 vote. Local enquiries revealed that the candidate in question does not belong to that area and nobody in the area seemed to know him, let alone vote for him.

***

The Elections to assembly and Lok Sabha were held simultaneously in Andhra Pradesh in April, 2009. A curious case of vote switching happened in polling station Number 73 in Rellivalasa village of Vizianagaram Parliamentary Constituency. In this polling station, the Congress candidate had secured only 11 votes in the Lok Sabha election and in the assembly election, the TDP had secured only 10 votes. Both these are highly improbable as these are the principal parties in the state. The unlikely beneficiaries are the BJP in Lok Sabha election, which secured 319 votes (against only 3 votes in assembly) and the BSP in assembly with 115 votes (against 7 votes in Lok Sabha).

Cases mentioned above in this chapter are only illustrative of the extensive reports originating from across the country about malfunctioning and suspected tampering of electronic voting machines. The Election Commission has been oblivious to such reports even when they were brought to its notice.

Need for Post-poll Audit

Various problems associated with the EVMs have

been highlighted in this chapter. Some of these could be due to technical glitches, while others offer clinching evidence of tampering of EVMs. No one comes to know about these glitches or deliberate election fraud because there is no attempt on the part of the Election Commission to carry out any post poll audit of the EVMs used in elections.

Post election audit refers to an in-depth examination of the accuracy of the voting process as a whole. With proper record keeping, an audit can facilitate a step-by-step examination of how a voting machine recorded cast ballots and computed vote totals to determine whether it performed accurately or not. An audit can examine any aspect of the election process that can be measured or recorded.

There has never been any post election audit on EVMs to understand the problems and the causes and magnitude of their occurrence. There is a dire need to document all cases of malfunctioning and misbehaviour of the EVMs and investigate them.

The Election Commission has not conducted any such audit or review till date because it believes that the ECI-EVMs are fail safe!! In the absence of such a systematic study, any assessment regarding the nature and magnitude of variations can only be a matter of speculation. But my estimate from various personal accounts is that it happens on a large scale.

Electronic voting machines (EVMs) are man made machines and are prone to errors. Further, they suffer from several technical vulnerabilities. EVMs used in Indian elections have gaping holes in their security and can easily be manipulated by miscreants; both from outside and inside as well. From various problems cited in this chapter, it is evident that hackers already appear to have done so. It is human tendency to exploit such weaknesses and security lapses. And, it is difficult to assume that several vices associated with Indian

elections earlier, like booth capturing have suddenly disappeared, post introduction of EVMs!

In the era of paper ballots, booth capturing became public knowledge whenever it happened. In the present electronic system, a meticulously planned and executed tampering operation in the EVM regime could go completely undetected, leaving no traces of evidence whatsoever. Beware, a perfect murder of democracy is possible! Only crude and failed tampering attempts would cause the EVMs to malfunction and misbehave as in several instances cited in this chapter.

As the muscle men exit the election scene, welcome the new breed of 'e-capturers' who are subverting people's mandate at will, via the electronic voting machines.

Electronic voting machines seem to have spawned a specialized breed of techies offering enterprising solutions to "fix" electronic voting machines.

5

Electronic Fixers Demand Hefty Sums

Is alleged tampering of electronic voting machines merely a figment of imagination or is there any truth in this? The answer to this question lies in personal experiences and encounters of a number of senior political leaders with "EVM fixers". From these personal accounts narrated by important and credible individuals, it is evident that there is more to the EVM story than what meets the eye. Take a look at some such shocking incidents narrated to me ever since I began to explore electronic voting machines in the wake of surprising election outcomes.

Insider "Fixing"

(Want EVMs fixed? Pay Rs. 5 Crore)

Weeks after elections to the state assemblies of Maharastra, Haryana and Arunachal Pradesh held in October, 2009, I met Omesh Saigal, a retired IAS officer and a whistle blower on the poor security of electronic voting machines.

"I was in Maharashtra in October. I met an ex-MP from the Congress party there. He confirmed my worst fears about EVMs", Saigal said.

"What did you hear from him", I queried.

"The ex-MP's son stood for the Maharastra assembly elections recently. The ex-MP told me that they were approached by some "authorised" engineers (apparently representing one of the EVM manufacturers or their agents) who offered to manipulate election results in 50% of the polling stations of his assembly constituency for the princely sum of Rs. 5 Crore. The engineers said that the candidate could choose whichever polling stations he wanted manipulated."


Omesh Saigal

"Scandalous. What happened then?" I asked Saigal.

"The ex-MP refused to believe them. He said that this couldn't be true. The engineers gave some (client) references to him and asked him to verify for himself, if he so desired", Saigal added.

Parties Scouting for Hackers

While the previous case referred to some 'authorised' technicians scouting for political clients to fix polls, there have also been some cases of political parties and candidates scouting for hackers to fix polls.


Hari Prasad

A few days after the notification was issued for October 2009 assembly polls, I received a call from Hari Prasad, managing director of a technologies firm, NetIndia based in Hyderabad.

"Today, some representatives of a prominent regional party came to meet us in Hyderabad. They said that they were aware that some techies from Hyderabad or Bangalore are "fixing"

elections in favour of parties and candidates. Can you do this for us?" Hari Prasad was asked.

"Gosh, that is unbelievable. Of all people, why did they approach you?" I asked Hari.

"They said that they did not know who exactly was involved in the tampering EVMs and were making discrete enquiries to locate the guys fixing polls." Hari said. "They seemed desperate to find the real hackers and were willing to pay any amount", Hari added.

Hari Prasad's firm had earlier developed a "look alike" EVM. He and his technical team along with V.V. Rao, the main petitioner who filed public interest litigation in the Supreme Court organized demonstrations at many places to show how easily EVMs could be tampered. That's perhaps why the regional party in question approached them for fixing elections.

"What did you tell them?" I asked.

"I told them that they came to the wrong guys. We know EVMs are vulnerable but can't help you in this regard. But, we can help you to educate your candidates and voters on EVMs by organizing training for them." Hari said.

"They (party representatives) seemed visibly disinterested in any such proposal. They were just looking out for techies who could fix polls for them", Hari informed me.

There were even more brazen attempts. NetIndia engineers were approached by some adventurous chaps from a small state seeking help in defeating a candidate from that state citing public interest as the motive. "They even sent us an email giving details, the techie who received the mail told me. They were promptly told that they couldn't be helped," Hari said.

Low Tech "Fixers"

While the above two incidents happened on the eve of assembly elections to Maharashtra, Haryana and

Arunachal Pradesh, many such stories began to circulate in the immediate aftermath of 2009 general elections.

A few days after the parliamentary election results, a State President of a national party that performed below its expectations told me, "Some engineers approached us offering to manipulate electronic voting machines to fix polls. They were very confident of manipulating results in our favour. We brushed them off as we did not take them seriously. Now, I shudder to think if our rivals had employed them."

The fixers in this episode met the party leader through a sitting Member of Parliament, who lost in 2009 Lok Sabha polls.

"The engineers approached me directly saying that they could tamper with the EVMs in select polling stations", the concerned ex-M.P told me later, after he lost his election.

"How would they do it?" I quizzed him.

"They said they would fix some wire manufactured by their associates in Mumbai in the EVMs at the ballot unit", the ex-M.P reported.

"Do these guys have access to the voting machines kept in secure environment?" I asked.

"No. They don't have access to the machines lying in the store rooms. They told us that they would train one voter selected by us in every polling station for tampering. He can enter the polling station as an ordinary voter and fix the wire as trained by them without getting noticed. All the votes thereafter would get polled in our favour" the ex-MP added.

"How many polling stations can they tamper for you?" I asked.

"They asked us to select about 100 to 150 weak polling stations in the parliamentary constituency where tampering of EVMs is to be done", the ex-MP added.

"How much money did they demand? I queried.

"They asked us for Rs. 20 Lakh for tampering EVMs in each Lok Sabha constituency" added the ex-MP.

Many such instances of 'election fixers' approaching party leaders and candidates have been narrated to me in the weeks that followed.

Types of Fixers

Electronic voting machines seem to have spawned a specialized breed of techies offering enterprising solutions to "fix" electronic voting machines. There are two kinds of fixers in the market as I gathered from various sources.

The first category comprises those who claim to be "authorised" engineers purportedly working on behalf of the EVM manufacturers. These people have free access to the EVMs and can play havoc with the election results. Given these strengths, they offer high cost, high precision services. The Maharashtra episode cited earlier puts this cost at a whopping Rs. 5 Crore per assembly constituency.

The second category is less sophisticated techies who offer fixing services at a much lower cost. They reportedly charge only Rs. 20 Lakh for each parliamentary constituency to fix elections in select polling stations. They adopt crude methods in tampering the EVMs in the polling stations. They would train one registered voter in each selected polling station who is a supporter of the candidate. On the polling day, he would enter the polling station to cast his vote as a common voter. Once inside the polling area, he would insert a jumper into the cable that connects the ballot and control units at the ballot unit end. It would take only a few seconds to fix the jumper. As the ballot unit is kept in a separate compartment, the polling officials wouldn't suspect any foul play.

A jumper is a short length of conductor used to close a break in or bypass part of an electrical circuit. The jumper is inserted at the ballot end into the cable that connects the ballot and control units such that all the votes would get registered in favour of the candidate in whose behest the election is to be fixed, irrespective of which candidate's button is pressed.

Voters wouldn't suspect any foul play as the ballot unit would continue to function normally and the LED next to the candidate's button would glow normally and a beep sound is heard from the control unit.

Tampering with the help of a jumper is possible only in the older EVMs. These old EVMs were extensively used in the parliamentary polls in several states. In the new/ upgraded EVMs used in select states, dynamic key coding logic doesn't allow such tampering. There are however, other tampering possibilities in the new and upgraded EVMs which contain separate microcontrollers in the ballot units.

Whatever I have cited above are personal experiences narrated to me by credible people. Admittedly, all the politicians referred above are those who have received such "offers". We have no confirmation from anyone who has actually engaged them to ‘steal’ elections. That is understandable. How can we expect anyone to own up one's own electoral fraud?

In the absence of such confessions or detection, whether the 'fixers' have indeed tampered with the EVMs used in elections can only be a matter of speculation.

One thing I can say for sure: this is not a 'con' job by crooks to make some fast bucks from unsuspecting and eager politicians. After all, would anyone dare to mess around with top politicians who are all powerful? Most likely not.

One might argue that the incidents narrated above may be isolated and rare cases. Let me inform you that

this is not the case. If you know any top ranking politician well, do find out. Chances are that he/she would have some such experience to narrate to you. In political circles, there is a strong buzz that techies are offering "EVM fixing" solutions to win elections.

Thanks to such experiences, after romancing with the EVMs for nearly a decade, most political parties in the country are now entertaining serious doubts about the reliability of the EVMs. The distrust among political leaders and parties, cutting across party lines and political divides, is so widespread that many of them are wondering if the integrity of election verdicts is safe anymore.

Much before I learnt about these insidious developments, the story of EVMs began to unfold for me on May 16, 2009 itself, the day election results were declared for 15th Lok Sabha. *How come, I wondered, no one expected the results of the 2009 general elections to be what they were?* Neither the winners nor the losers had any clue about the final outcome. The same is true of the media, pollsters and the international community. Lest you forgot the "real" happenings at the time, I have narrated in chapter 6 the sequence of events and the uncertainty that gripped the nation in the run up to the 2009 general elections.

Is there something esoteric and mysterious in the fact that the only two parliamentary elections in India's parliamentary history, where the pollsters in general have gone horribly wrong, were totally 'electronic' elections in which electronic voting machines (EVMs) were used all over the country?

6

The X-Factor

"Anything that is unexpected is the X-factor."
Dante Hall, American football player

May 16, the D Day

May 16, 2009 was a very important day in the political history of the country; the day when the election results were to be declared for the 15th Lok Sabha, India's lower house of parliament. It was the D-Day for scores of political leaders and prime ministerial aspirants as also for contestants vying for the membership in the nation's most coveted club, the Indian Parliament.

With their fate already sealed in the electronic voting machines and having completed their mandatory reviews, all of them had only one thing left to do. Hope. Hope for the best outcome. Yet, no one was sure. At least not this time. They anxiously waited for the morning of May 16 for the counting of votes and declaration of results.

Even as no party or pre-poll alliance appeared confident of victory, no party felt that it was out of the reckoning. Hope was writ large on every leader's face

and even regional satraps with only a modicum of strength began to fancy their chances of making it to the highest office of the land, the exalted office of the prime minister.

There were many other minor players who were readying to perk up their demands in return for support for government formation. After all, the deals struck in the run up to the confidence vote in July, 2008 to save the Manmohan Singh led United Progressive Alliance (UPA) government at the Centre, after the withdrawal of support by the left parties, were still fresh in their minds.

A repeat of the unsavoury events witnessed in the run up to the Manmohan Singh Government's trust vote win appeared to be on the cards, and for the political parties the political 'bazaar' never appeared so attractive. The impending election outcome in the form of a hung verdict appeared to be yet another dream run that would make every minor party relevant and every newly elected Member of Parliament a prized catch. So, everyone thought.

The five phases of polling for the 15th Lok Sabha which ended on May 13 saw a vicious election campaign unleashed by political rivals. Even as the parties were busy fighting what appeared to be the most fiercely fought election in the recent memory, simultaneously, they began hectic lobbying and back channel manoeuvrings to clinch the outcome of the election in what was amusingly billed as the 'sixth phase' of elections i.e political deal making after the declaration of election results on May 16. There appeared to be near unanimity among all-the political leaders, independent political analysts and observers – that the country was heading towards a simmering season of sizzling political deals.

Unsure Congress

A number of actions and statements by the members of the Congress party's first family, the Nehru-Gandhi

household, in the run up to the parliamentary election reinforced the perception that the country was headed for a splintered verdict and that no party or alliance, not even the Congress party led United Progressive Alliance (UPA), was comfortably placed in the electoral sweepstakes.

In a much publicized press conference on May 5, after more than two thirds (372 of the 543) of the parliamentary constituencies had already voted in the first three phases of polls, Rahul Gandhi betrayed signs of nervousness as the polling process was drawing to a close. In an unusual twist to the developing sordid political drama, Rahul Gandhi showered fulsome praise on the Congress party's sworn political rivals such as the Telugu Desam Party (TDP) leader N. Chandrababu Naidu, Bihar Chief Minister Nitish Kumar and subtly hinted that his party was willing to work with them in the post poll scenario. Nothing appeared to be coming in the way of soliciting support.

10 days to go, Rahul reaches out to rivals

MAY 6: The first leader from his party to do so openly, Gandhi praised rivals Nitish Kumar of the JD (U) and Chandrababu Naidu of the TDP, and talked about the Congress's common ground with the Left. This was clearly a bid to isolate the BJP, undercut the Third Front and project the Congress as the pivot of a coalition after the results come in on May 16.

At an hour-long press conference before the fourth phase of polling on Thursday, Gandhi claimed the Congress was not going to sit in Opposition, claiming that the party would be the only option for regional parties after May 16. (Indian Express, May 7, 2009)

The message from Rahul Gandhi's press conference was loud and clear: there were no permanent rivals in politics and anyone having a few seats in Parliament is a valued friend in these uncertain times.

At that time, party and political circles were abuzz with rumours that the Gandhi parivar was making last ditch efforts for the Congress party to lead the next government after the polls and should the attempts fail – which the party considered to be a distinct possibility – Rahul Gandhi would be anointed Leader of the Opposition in the Parliament to prepare him for a prime ministerial bid in 2014.

Evidently, there was growing unease in the Congress party's first family about the impending election outcome and the 'crown prince' of the Congress party was himself proving to be a bundle of nerves.

Another instance of the Gandhi household's pre-poll jitters was evident from Priyanka Gandhi Vadra's interview to the Outlook magazine. In the interview published in the magazine's May 11, 2009 issue just days before the declaration of election results, Priyanka was asked as to what her prediction was for the Congress party in the election. Her reply was candid and matter of fact. She said, "I think this election is very touch and go. Touch and go in the sense that it is going to be a close call."

In the Outlook interview, Priyanka had this to say about Rahul, *"During the last elections (2004), the only one who had the numbers exact was my brother. All the rest of us thought we were not going to do well, but he was very clear right from the beginning, and he had all the numbers and papers lined up and they were actually pretty accurate".*

Sonia Gandhi, mother of Rahul and Priyanka, is the party's undisputed leader of the Congress party. To her credit, Italy born Sonia has come a long way in her political career and breathed life into the moribund Congress party. At a time when most people had written

off the Congress party, Sonia's strategy of striking astute electoral alliances, combined with a quirk of circumstances brought the Congress party back to power at the Centre in 2004, defeating a seemingly invincible Atal Bihari Vajpayee led National Democratic Alliance (NDA) regime at the Centre. With her party's victory in 2009 polls, Sonia has given her party stunning back to back victories in parliamentary elections in the face of a strong anti incumbency sentiment.

Throughout the campaign for the 2009 parliamentary election, Sonia was circumspect and unlike her children, did not reveal her mind on the impending election outcome. Was Sonia confident of a favourable election outcome? No. Being more cautious and guarded by nature, she spoke nothing. But, Sonia, like her children, was on pins and needles about the election outcome.

Highly placed Congress sources at the time revealed that one action by Sonia clearly showed that she was jittery. She had got the Manmohan Singh government to withdraw the Interpol's Red Corner Notice (RCN) against Ottavio Quattrocchi, an Italian businessman and a family friend. As they say, deeds speak louder than words. (See Box on the next page)

Alliance hopping

The run up to the 2009 general elections saw parties deserting the two principal alliances, namely the Congress party led United Progressive Alliance (UPA) and the Bharatiya Janata Party (BJP) led National Democratic Alliance (NDA). In the two months preceding the Lok Sabha election, many time tested alliances broke apart from their long term friends.

On the eve of 2009 polls, most of the regional parties reckoned that neither the Congress nor the BJP would be able to capture power at the Centre as the prospect of a hung Parliament loomed large. Regional parties

In last days of UPA govt, Quattrocchi is off CBI's wanted list

April 28: With just three weeks to go before the Congress-led UPA government's term ends, Ottavio Quattrocchi, the lone surviving suspect in the Bofors payoff case, no longer figures in the Central Bureau of Investigation (CBI)'s list of wanted persons. The 12-year Interpol Red Corner Notice (RCN) against the Italian businessman has been taken off the "Interpol Notices" section of the agency's website.

Sources have confirmed to The Indian Express that last week Minister of State for Personnel Prithviraj Chavan and Law Minister Hansraj Bhardwaj held meetings with the CBI Director on the issue. When contacted, Chavan said: "I will have to find out what the position is. The agency is doing independent work." (Indian Express, April 29, 2009)

deserting the UPA and the NDA preferred to keep their options open or join the third front to enhance their bargaining power in the post-poll scenario. The emergence of the Third Front, a conglomeration of regional parties joined by the left parties and a Fourth Front, comprising regional, caste based parties in the cow belt took shape only weeks ahead of Lok Sabha polls.

The BJP led NDA that ruled at the Centre between 1999 and 2004 had as many as 23 parties as its constituents. The Congress led UPA government, which came to power in 2004, was also a large conglomeration with a number of parties either joining it or supporting it from outside. Thus, in the last decade, India was ruled by coalition governments, either led by the Congress party or the Bharatiya Janata Party (BJP).

The sudden political activity and realignments preceding the 2009 Lok Sabha polls signalled that the coalition era, which took root in the past decade, was here to stay as no single party, be it the BJP or the Congress, had the electoral strength and appeal to acquire a big tally on its own.

The BJD Shock

The rival challenger to the Congress led UPA, the BJP led NDA suffered the first blow with the exit of the Biju Janata Dal (BJD) led by Naveen Patnaik, a long time BJP ally and a member of the NDA, who deserted the alliance barely weeks before the simultaneous polls to the Lok Sabha and the Orissa state assembly. Though there were some early signs that a break-up may be in the offing, the wily Patnaik who had made up his mind much earlier, kept the BJP guessing until the last moment and dumped it after making all his preparations.

What was it that made a risk averse Patnaik bold enough to desert the BJP unceremoniously? Around the time the break up happened, there were reports, not entirely unfounded, that the Congress party had a hand in the developments. The Congress party's managers had apparently conveyed to Patnaik through their BJD friends in Delhi that the national party was willing to offer a quid pro quo deal: it would extend support to Naveen Patnaik in case he fell short of numbers in the assembly in return for the BJD's support to a Congress led government at the Centre. The manner the Orissa unit of the Congress allowed the BJD government to survive immediately after the BJP had withdrawn its support to the Naveen Patnaik government in March 2009 lends credence to this theory of a clandestine arrangement between the erstwhile arch rivals in Orissa.

The Congress party was willing to forsake its interests in the state of Orissa by sewing up a covert

alliance with its arch political rival for two decades, the Biju Janata Dal (BJD). The Congress party reckoned that a break-up of the BJD-BJP alliance would push the NDA tally down by a minimum of 15 to 18 seats and that was a large number that the NDA would find impossible to make up for elsewhere.

Expectedly, the BJP suffered heavily from its split with the BJD. Besides losing a crucial state like Orissa, it made the BJP led NDA's challenge look much weaker. As it is, for want of viable election alliances, the NDA was a non starter in several battleground states like Andhra Pradesh, West Bengal and Tamil Nadu accounting for as many as 123 states in the Lok Sabha. The loss of Orissa, a BJD-BJP bastion, which had delivered a rich harvest in successive Lok Sabha elections since 1998, cost the NDA dearly.

The Congress party's covert support to the BJD had a strategic intent. The party, unsure of a strong performance at the national level, apparently believed that weakening the rival NDA was a way to keep its hopes of recapturing power alive.

UPA Deserters

The Congress party revelled in the discomfiture of the rival NDA camp at the exit of the BJD. It had little idea that there would be desertions from its own camp soon there after. Lalu Prasad Yadav led Rashtriya Janata Dal (RJD) and Ram Vilas Paswan's Lok Janshakti party (LJP) abandoned the United Progressive Alliance (UPA) barely weeks before elections.

RJD and the LJP, two Bihar specific regional parties along with the Mulayam singh Yadav led Samajwadi party (SP) came together to form a 'fourth front'. Both the RJD and the LJP were members of the UPA coalition since

2004 and participated in the Manmohan Singh government holding key ministries. The Samajwadi party – despite its crucial support to the Manmohan Singh government in the 2008 confidence vote in Parliament which helped it to survive after the withdrawal of support by the left parties – had given up on the Congress party for getting too ambitious with its seat sharing demands without having enough support base in the state of Uttar Pradesh.

The RJD and the LJP humiliated the Congress party by unilaterally deciding to contest 37 of the 40 parlia-mentary seats in Bihar, leaving merely three seats for the national party and head of the United Progressive Alliance (UPA). The Congress party pleaded with Lalu Prasad Yadav to offer it a more respectable number of seats. Political sources at the time revealed that the Congress party had demanded eight seats but would have settled for even six seats to keep the alliance going.

But, Lalu Prasad was in no mood to relent. He argued that he could not give more than three seats to the party and there could be no reconsideration of his party's decision. It was a 'take it or leave it' offer and not one of accommodation which usually marks such electoral negotiations.

Both Lalu Prasad Yadav and Paswan are grassroots politicians and would not have treated the Congress party in a cavalier manner if they had even an inkling that the Congress party would comfortably return to power at the Centre. In a sense, they both dumped the Congress party on the eve of elections to keep their post election options open.

Alliances in Fray

Thus, four pre-poll rival alliances were in the fray in the 2009 general elections. They were the

ruling Congress party led United Progressive Alliance (UPA); its principal challenger, the Bharatiya Janata Party (BJP) led National Democratic Alliance (NDA); the left parties' led Third Front comprising of disparate regional parties; and the fourth front comprising the Mulayam Singh Yadav led Samajwadi party (SP), the Rashtriya Janata Dal (RJD) and the Lok Janshakti party (LJP).

One thing was clear to all: that no pre-poll alliance – neither the one led by the Congress party nor the BJP nor any other – was likely to be anywhere close to winning a majority of 272 seats in the 543 member Lok Sabha.

NDA's Accretion of Strength

On May 10, the NDA organized a massive rally in Ludhiana to exhibit its strength and unity. Organised by the NDA ally, the Shiromani Akali Dal led by Prakash Singh Badal, the NDA used the Ludhiana event to send out a signal that it was brimming with confidence about its electoral prospects. This became necessary after Rahul Gandhi made a desperate attempt to poach in the rival NDA camp by praising Nitish Kumar, Bihar chief minister and long standing ally of the BJP in his press conference on May 5.

Nitish Kumar, the favourite target of the Congress party, attended the Ludhiana rally and his bonhomie with the BJP's leaders put paid to all intelligently motivated propaganda that he was likely to support a Congress party led dispensation at the Centre.

The big surprise of the Ludhiana rally was the participation of K. Chandrasekhar Rao, Founder and President of the Telengana Rastra Samiti (TRS). TRS fought elections as a member of the Third Front in alliance with the Telugu Desam Party (TDP) and the left parties in Andhra Pradesh.

With less than a week to go for elections, when most

parties preferred to keep all their options open, Rao's decision to support the BJP led NDA just days before the declaration of results was seen as a shot in the arm for the NDA and augured well for its government formation efforts.

US Envoy meets Indian leaders

The suspense regarding the 2009 election outcome gripped not just India's political leaders and its electorate; even the international community appeared to be anxious about the outcome, particularly due to the unusual division witnessed in the Indian political class over the Indo-US Civilian Nuclear Agreement, popularly known as the Indo-US nuclear deal.

IBN Live

US diplomat's meetings trigger political row

May 14, 2009

New Delhi: A US diplomat's meetings with Indian political leaders at the fag end of the Lok Sabha elections has sparked a row with the Left Thursday accusing Washington of meddling in New Delhi's internal affairs and the US embassy denying the charge.

The US embassy said that no political meaning should be read into the meetings. 'He (Burleigh) met with (Chandrababu) Naidu for routine consultations. The US categorically denies any attempt to interfere in India's democratic political process,' a spokesperson for the US embassy said.

The US is closely watching the Indian election, which is expected to produce a fractured mandate.

With the Left fiercely opposed to the India-US nuclear deal and the larger strategic relationship between the two countries, there is concern in Washington about the Communists wielding influence in the next government.

The Communist Party of India (Marxist) led Left Front had withdrawn support to the Manmohan Singh government earlier in July 2008 due to ideological differences with the Congress party over the signing of the nuclear deal. The nuclear deal became a reference point for realignment of political forces into pro and anti nuclear deal camps. The nuclear deal had acquired a high degree of salience in Indian politics and the BJP and the left parties, with diverse ideological positions, appeared to be on the same side of the nuclear deal debate, though for entirely different reasons.

In the backdrop of these developments, the 2009 Lok Sabha election became a subject matter of great interest to the United States and other countries that have a stake in the continuation of the nuclear deal. What would be the fate of the already inked Indo-US Civilian Nuclear Agreement in case the Congress party failed to return to power, they wondered? Thus, American Embassy in Delhi was anxious about the election outcome and its implications for the nuclear deal.

Barely a few days before the election results were to be declared, the US Charge d' Affaires. A Peter Burleigh met with the BJP's Prime Ministerial candidate LK Advani in New Delhi and the Telugu Desam Party (TDP) Chief, Nara Chandrababu Naidu and Praja Rajyam party Chief and actor Chiranjeevi in Hyderabad.

Though what transpired in these meetings is unknown, the speculation was that a worried American administration was trying to understand how these parties would approach the nuclear deal; how the events were likely to unfold after the declaration of results and what their implications would be for the Indo-US relations.

I am citing this incident to highlight that even the international diplomatic community, which generally has a good fix on ongoing political developments, had

widely anticipated a fractured mandate and an inclement political weather post elections.

***

The Countdown, May 16

9 A.M

The initial trends began to flash on television screens and they showed the Congress party performing much better than expected in a number of states. These were early trends but pointed towards a sizeable lead for the Congress party. Are these early trends reliable? Early reporting is usually based on the initial trends from a very limited number of polling stations. From my TV broadcasting experience, I knew it would take at least an hour for constituencies to report firm trends based on a reasonable progress of counting. The trends, however, began to consolidate in favour of the Congress party as the counting progressed. But, many states were still to report trends as the counting process is slow in some states.

10 A.M

The election results began to look firm as all states had started reporting by this time. The Congress party and its allies were sweeping the polls in the Southern states, except Karnataka (where the BJP held sway) and were even leading in battleground states like Maharashtra and West Bengal. It became clear that the BJP led NDA lost out in the race due to severe electoral setbacks it received in north Indian states like Uttar Pradesh, Rajasthan, Haryana, Delhi and Uttaranchal. The Congress led UPA seemed to have the momentum. Yet, it didn't appear to be heading towards a majority of its own.

11 A.M

The election trends came as a huge disappointment for the principal challenger, the BJP led NDA. The BJP

conceded defeat by 11 A.M. L.K. Advani, the prime ministerial candidate of the NDA congratulated the Prime Minister Manmohan Singh on the Congress party's stunning victory. Prakash Karat, General Secretary of the Communist Party of India (Marxist) and the principal architect of the third alternative to the Congress and the BJP conceded defeat by the afternoon after the trends showed that his party and the left front had suffered major setbacks in both Kerala and West Bengal, considered to be red bastions.

***

The After Shocks

Proving its own assessments wrong, the Congress party won a stunning victory by winning as many as 206 seats (up from the 145 seats it won in the 2004 polls) and a near majority in parliament for its United Progressive Alliance (UPA) by winning 263 seats in the 543 member house, just nine short of an absolute majority. *The Lok Sabha election results stunned the Congress leaders as much as they stunned its rivals.*

None of the key players – political leaders, media, poll pundits, diplomats etc. – had had any inkling about the final election result: a near majority for the UPA and a whopping tally of over 200 seats for the Congress party. Nor had anyone expected the opposition to be trounced so badly.

The BJP and the Left Front suffered their worst electoral defeats in many decades. Regional parties that had weathered many a political storm and survived and thrived at all times did not know what catastrophe struck them. All these parties were utterly unprepared for the electoral Tsunami that hit them and swept them away. In a span of just three hours, an electoral earthquake that hit the Indian political coast, perhaps the biggest and the most unexpected ever, left a trail of devastation.

May 16 was a day that shattered many dreams. The

conjured images of a hung parliament that appeared to be the hallmark of 2009 election until that morning proved to be unreal and illusory. The much anticipated "6th phase" of elections that was expected to see intense jockeying and bargaining also proved to be a chimera.

***

Exit Polls Go Awry

Exit polls did no better. All the 'Exit polls' estimated that the best performing alliance was likely to be afar by nearly 50 seats from securing a simple majority of 272 seats in the 543 member Lok Sabha. After the 2004 Exit poll fiasco, once again, the media polls completely missed the Congress surge in 2009 Lok Sabha polls.

E-Voting Fails Exit Pollsters

The track record of exit pollsters in India was remarkable until 1999. My own projections for successive Lok Sabha elections in 1996, 1998 and 1999 were spot on. Why is it that the Indian pollsters have failed to read the voter mood correctly in the 2009 and 2004 Lok Sabha elections when they were able to do so very accurately until 1999? (Refer Table at the end of this chapter)

Is there something esoteric and mysterious in the fact that the only two parliamentary elections in India's parliamentary history, where the pollsters in general have gone horribly wrong, were totally 'electronic' elections in which electronic voting machines (EVMs) were used all over the country?

Ever since Indian elections went electronic with the nation-wide use of electronic voting machines, voting patterns have become extremely unpredictable. The results of 2004 and 2009 parliamentary elections and the recent elections to the state assemblies of Maharashtra and Haryana bear out this assessment. That leads us to ask the natural question: are the

electronic voting machines responsible for the jerky election outcomes in Indian elections? In other words, do EVMs constitute the enigmatic 'X factor' in the recent Indian elections?

A series of questions kept coming to me in quick succession as election after election began to surprise all, including the voters. Are the EVMs reliable? Do they record votes accurately? What has been the experience of the common voters in using EVMs?

The **Star News-Nielsen Exit poll** predicted a hung Parliament and a close fight between the Congress-led UPA and the BJP-led NDA. The survey gave 202 seats to the UPA and 198 seats to the NDA. The Exit poll projected a close race for the single largest party status giving 157 and 154 seats respectively for the Congress and the BJP.

The **NDTV Exit Poll** predicted that the Congress-led UPA would emerge well ahead with 216 seats, followed by the NDA (177 seats), Third front (105 seats) and the Fourth Front (30 seats). The Exit poll forecast 160 seats for the Congress party.

Exit poll by the CNN-IBN TV News channel initially gave 185-205 seats for the UPA and 165-185 seats for the NDA. Barely a few hours before the counting began for the 2009 Lok Sabha elections, the CNN-IBN News Channel revised its projections giving the Congress led UPA 210-225 seats in the 543 member house and 165 seats for the Congress party.

The Times of India-Times Now TV News channel came up with political assessment reports based on extensive inputs received from their correspondents around the country. Its projections: 198 seats for the Congress party led UPA and 183 seats for the BJP led NDA. It gave 154 seats for the Congress and 142 for the BJP.

1:EXIT POLL PROJECTIONS: LOK SABHA ELECTION, 2009				
TV Network	**Total**	**BJP+**	**Congress+**	**Others**
Star News	543	198	202	143
NDTV	543	177	216	150
CNN-IBN (First)	543	175	195	173
CNN-IBN (Final)	543	188	218	137
Times Now*	543	183	198	162
ACTUAL RESULTS				
ALL INDIA	543	159	263	121

2:EXIT POLL PROJECTIONS: LOK SABHA ELECTION, 2004				
TV Network	**Total**	**BJP+**	**Congress+**	**Others**
Sahara Samay	543	270	176	97
Star News	543	270	181	92
Aaj Tak	543	248	189	106
Zee News	543	249	176	118
NDTV	543	240	197	106
ACTUAL RESULTS				
ALL INDIA	543	185	217	141

3: Exit Poll Predictions (1996, 1998, 1999)†			
Lok Sabha Election	**Alliance**	**Projection**	**Actual**
1996	BJP+	188	189
	Congress+	142	132
	Others	212	215
1998	BJP+	252	252
	Congress+	140	147
	Others	145	138
1999	BJP+	287	298
	Congress+	174	135
	Others	77	105

** Political Assessment*

† Poll prediction by G.V.L. Narasimha Rao for Times of India/ Doordarshan; Source: Indian Elections in Nineties by GVL Narasimha Rao and K. Balakrishnan (Published, 1999)

For the first time since the nationwide introduction of EVMs in 2004, a number of parties began to wonder if the EVMs could have cost them the election. The concerns regarding the EVMs were widespread and cut across the entire political spectrum.

7

Vote of No Confidence

"The Democrats think Republicans are stealing elections. The Republicans think Democrats are stealing elections. And, those of us who are neither, know they are both right."

Kevin Zeese, American Political Activist

The Lok Sabha election results had shocked both the winners and the losers, though understandably in different ways. The 2009 parliamentary election, after a gap of exactly two decades, truly saw a resurgent Congress occupy centre stage in the national politics. The Congress party – with its unexpected tally of 206 seats in the election – surpassed its own expectations. The accretion in Congress party's parliamentary strength was dramatic and meteoric.

Losers' Consternation

The unexpected scale of defeat had caused consternation among the parties which had performed much worse than their expectations. Most of the leaders of the losing parties – this included leaders of the BJP, left parties or regional parties – had an eerie feeling that something had gone wrong with the elections. No one exactly knew what.

Nonetheless, for the first time since the nationwide introduction of EVMs in 2004, a number of parties began to wonder if the EVMs could have cost them the election. The concerns regarding the EVMs were widespread and cut across the entire political spectrum. Even the Congress party that had spectacularly won the 2009 polls had serious apprehensions that it had lost in Orissa because the EVMs were manipulated in that state by its political rivals.

"The Purpose of voting technology is to record and tally all votes accurately and to provide sufficient evidence to assure all participants-especially the losing candidates and their supporters-that the election results accurately reflects the will of the voters."

Jimmy Carter & James Baker III

Congress's Complaints

At a press conference in Bhubaneswar on June 18, 2009 Ghulam Nabi Azad, Congress party's general secretary in charge of Orissa and present Union Health minister alleged large scale manipulation of EVMs by the ruling Biju Janata Dal.

The Congress party had its own reasons to be suspicious. In the state of Orissa, in simultaneous assembly and parliamentary polls, the Congress party had won a paltry 27 of the 147 assembly seats and six of the 21 Lok Sabha constituencies.

The ruling party, Biju Janata Dal (BJD), led by Chief Minister Naveen Patnaik –BJD fought elections alone following its split with the BJP – swept the polls winning 103 assembly and 14 Lok Sabha seats.

HEADLINES INDIA™
.com
CURRENT, CREDIBLE, CONSISTENT NEWS

Voting machines 'manipulated' in Orissa polls: Azad

Thursday, June 18, 2009

Bhubaneswar: Congress general secretary in charge of the party's affairs in Orissa Ghulam Nabi Azad today alleged "manipulation" of electronic voting machines (EVMs) had led to the party's defeat in the assembly and parliamentary elections in the state.

"EVMs were manipulated during the poll which resulted in defeat of many Congress candidates," Azad said in a press conference here.

Azad met the candidates in the twin polls and reviewed the reasons of dismal show, constituency wise. After the review meeting, he also charged the BJD with misusing the official machinery during the polls.

"There was a wide-scale misuse of official machinery by the ruling BJD, which led to the debacle of the Congress party in the poll," he alleged. (IANS)

In 2009 Lok Sabha polls, the Congress party had registered vote gains in most states where it is in the opposition. Surprisingly, it suffered a loss of eight percentage points in votes in Orissa and its vote share dropped from 40.4 per cent to 32.8 per cent. This is the lowest vote share ever polled by the Congress party in Orissa in parliamentary polls.

There were no apparent reasons as to why a nationally resurgent Congress party should suffer losses in a state where the party had been out of power for a decade. Following widespread complaints that the EVMs malfunctioned during polls due to their tampering, the Congress party leaders filed an election petition in the Orissa High Court. The petition alleged large scale

tampering and manipulation of EVMs by the ruling Biju Janata Dal.*

DNA
Read the world

Congress blames BJD of EVM tampering in Orissa

PTI

Wednesday, June 17, 2009 23:47 IST

Bhubaneswar: Maintaining that free and fair election would have taken place under Central rule, some Congress leaders accused the ruling BJD of manipulating EVMs, misusing government machinery and even poll officials, state Congress media cell chairman Kailash Acharya told reporters.

"It was felt that replacement of several EVMs at many places in a fraudulent manner and bogus voting led to defeat of a large number of Congress candidates," he said.

Many Congressmen claimed though there was no visible wave in favour of BJD, the party scored a landslide victory through rigging and manipulation of EVMs, Acharya said.

L.K. Advani's Apprehensions

Two weeks after the Congress party voiced its apprehensions on Orissa mandate, L.K. Advani, NDA's prime ministerial candidate expressed doubts about the reliability of the EVMs. L.K. Advani was, however, gracious and careful not to make allegations like rigging or malpractices in the elections.

Lal Krishna Advani (82) is a tall national leader and was deputy prime minister in Atal Behari Vajpayee government at the Centre. He was the Leader of the Opposition in the 14th Lok Sabha and the NDA's prime ministerial candidate in the Lok Sabha polls.

* *See Annexure 7*

Advani is a widely respected parliamentarian and the quintessential organization man credited for the ascendance of the Bharatiya Janata party (BJP) in national politics and for its emergence as an alternate pole to the Congress party in national politics.

Advani has doubts about EVM, wants ballot papers back

Suman K Jha
Sunday, Jul 05, 2009

BJP leader L.K. Advani has demanded the reintroduction of ballot papers in elections, beginning with the Maharashtra Assembly elections in October, and three other states later this year.

"We should revert to ballot papers unless the Election Commission is able to ensure that Electronic Voting Machines (EVMs) are foolproof and every possibility of their malfunctioning is taken care of," Advani told The Sunday Express here on Saturday.

Citing the instances of Germany (which has banned electronic voting altogether) and the US (which has elaborate guidelines for voting through EVMs), Advani stressed that "no one was raising any questions like rigging or malpractices in the elections", but larger questions about the "possibility of EVMs' malfunctioning...must be addressed".

After the recent elections, some state units of the BJP had leveled allegations of "malpractices through EVMs". The issue also figured in a meeting of the BJP's newly-elected MPs last month.

Advani has a habit of telling it like it is. He applies his mind on all important issues and reflects on them before making his views public. He measures his words carefully and presents his views in a lucid and succinct manner and does not tend to obfuscate issues.

Though L.K. Advani raised his concerns on EVMs many days after other leaders like Ghulam Nabi Azad (Congress), Chandrababu Naidu (Telugu Desam Party) and Jayalalithaa (AIADMK) had aired them, the EVM debate had acquired urgency and national prominence only after L.K. Advani spoke about it.

The After Shocks

L.K. Advani's views had brought the subject of EVMs onto the centre stage. So significant and compelling were Advani's views that even parties that have a strong adversarial relationship with the BJP like the Communist Party of India (Marxist), Rashtriya Janata Dal (RJD), Lok Janshakti Party (LJP), Janata Dal (Secular) have instantly endorsed Advani's apprehensions.

In all this, it appeared as though a consensus was developing on the need to review and remedy the present voting system. The number of parties having serious misgivings about the EVMs continues to swell.

Communists Express Reservations

Echoing the apprehensions expressed by L.K. Advani, CPI (M) Polit Bureau member Sitaram Yechury said, "Many questions have already been raised relating to the EVMs. These are serious issues and if we want to strengthen our democracy, then we should consider the matter very seriously.'' Noting that many developed countries have reverted to ballot papers, Yechury felt that there was a need to reconsider options. He even called for a probe into charges of malfunctioning of EVMs in many places.

Prakash Karat, CPI (M) General Secretary, in a letter to the Chief Election Commissioner Navin Chawla dated September 1 wrote, "In the recent period, a number of questions have been raised about the reliability of the EVMs in the polling process. Amongst the concerns is the possibility of tampering with the program chip embedded in the EVMs and further the lack of any verifiable record of the vote cast by a voter".

Communist Party of India (Marxist)

Memo to the Election Commission

7 September 2009

Questions on reliability of EVMs:

1. Possibility of incorporating a Trojan horse into the chip.
2. Possibility of manipulation of chips during manufacturing, insertion and transportation stages.
3. Lack of EC control on the entire technical process of the EVMs.
4. Lack of third party check/inspection/guarantee on the programming of the chips used in the EVMs.
5. Banning the usage of EVMs in some Western countries particularly in Europe.
6. Reporting of errors in some machines and the discrepancies in the results.

Steps that need to be taken to restore the confidence of the political parties and people on the usage of the EVMs:

1. The entire manufacturing process has to be done under the control of the Election Commission and for this an exclusive technical department needs to be established.
2. Both hardware and software should be in public domain.
3. The chips manufactured by ECIL, BEL should be allowed for yearly random third party inspections either by NIC or IITs.
4. All the machines should be randomly changed from state to state and within the country in every election.
5. A verification tool should be developed and made available to all.

Adding that many countries, having the requisite technological know-how had stopped the use of EVMs or prescribed conditions for their use, Karat wrote, "It is important that all doubts about the use of the EVMs for voting are removed, so that people's faith in the democratic system is not affected".

Karat, a no-nonsense politician, demanded that the poll panel should hold a meeting of all parties and technical experts to clear doubts and allay apprehensions about the use of electronic voting machines. The Election Commission refused to oblige Karat and his demand for an all party meet remains unheeded. However, the Election Commission invited Prakash Karat for a discussion. Prakash Karat and his fellow comrades met the Commission on September 7, 2009 and submitted a memo highlighting their concerns.

Southern Discomfort

Well before L.K. Advani and Prakash Karat voiced their concerns on EVMs, southern regional satraps led by Telugu Desam party (TDP) chief, Chandrababu Naidu in Andhra Pradesh and the All India Anna Dravida Munnetra Kazhagam (AIADMK) Supremo, Dr. J. Jayalalithaa of Tamil Nadu articulated their vehement opposition to the electronic voting machines.

Chandrababu Naidu and Jayalaithaa were the first to fire salvos against the EVMs alleging that they were susceptible to rigging. Both the leaders demanded that the Election Commission of India (ECI) should junk the EVMs and return to the old ballot paper system to ensure that the people's voting choices are properly registered.

Tech Savvy Naidu Says No to EVMs

N. Chandrababu Naidu, former chief minister of Andhra Pradesh, is indisputably India's first techno savvy and laptop-toting politician. Naidu had captivated the entire political class with his abiding interest in IT. This coupled with his professional approach to politics and

governance had earned Chandrababu Naidu, when he was the state's chief minister, the epithet of Chief Executive Officer (CEO) of Andhra Pradesh.

Naidu is convinced that the electronic voting in the present form practiced in India is unreliable and must be jettisoned. Though a passionate enthusiast of information technology, he never tires of highlighting the dangers of electronic voting.

Jayalalithaa Boycotts By-Elections

Even as the polling for parliamentary election was underway in Tamil Nadu, the AIADMK General Secretary, Dr. J. Jayalalithaa aired her concerns over the malfunctioning of the EVMs. Jayalalithaa told the media on May 13 – the day all the 39 parliamentary seats in Tamil Nadu went to polls – "In many polling stations in Tamil Nadu, EVMs are not functioning properly. Even votes polled in favour of the AIADMK are being registered in favour of other candidates."

The AIADMK and its ally, the PMK believed that the Lok Sabha polls in the state were 'fixed' to deliver false victories to their rivals. Jayalalithaa had demanded that the Election Commission must jettison EVMs in the by-elections scheduled to the five assembly constituencies in the state on August 18, 2009 three months after Lok Sabha polls. When the Commission refused to heed the suggestion, AIADMK boycotted the by-elections.

Predictably, Jayalalithaa's accusations that the EVMs were tampered in Tamil Nadu rattled the Election Commission and prompted it to use the new, upgraded electronic voting machines in the by-elections in the

state in place of the old EVMs used in Lok Sabha elections in Tamil Nadu.

Like Naidu, Jayalalithaa also believes that a physical record of voting is necessary to give confidence to the voter that her/ his vote had been recorded properly. Says Jayalalithaa, "In a democracy, every voter has a right to know whether the vote she/ he has cast has gone to the candidate or party it was meant for. In the absence of such certainty, the entire democratic process will be rendered a mockery".

Ever in Power PMK Smells a Plot

Pattali Makkal Katchi (PMK), a regional party in Tamil Nadu founded by Dr. S. Ramadoss strongly opposes the EVMs. The PMK was an ally of the DMK and a constituent of the UPA at the Centre until the announcement of Lok Sabha polls. The PMK switched to the rival AIADMK on the eve of 2009 Lok Sabha polls.

The regional party had switched effortlessly before every election in the last decade between the rival Dravidian parties, the Karunanidhi led DMK and the Jayalalthaa led AIADMK. But it always ended up being in the victor's camp. The widely held notion in the political circles was: wherever the PMK goes, the alliance emerges the winner as the party had an uncanny ability to read the public mood and pick the winner. The PMK draws support heavily from the Vanniar caste and has secured a minimum of four Lok Sabha seats in the previous three Lok sabha elections. This time around, however, the PMK proved to be unlucky and drew a blank in Lok Sabha polls.

The PMK leaders believe that the electoral rout was the result of fixing of EVMs by its political rivals. Unable to accept the verdict, the PMK filed a writ petition in the Madras High Court alleging that the EVMs were tampered in Lok Sabha elections in Tamil Nadu. Madras

High Court directed the petitioners to approach the Election Commission to air their grievances.

In their petition to the Election Commission, the PMK representatives wrote: "(U)nder the electronic voting system, *neither the election agents nor the voters have the facility and satisfaction of scrutinizing the ballot-boxes and ballot-papers prior to and during the casting of vote. And there is no physical reconstruction of the vote in case of dispute. These deficiencies have severely eroded voter's faith in the electronic voting system,* despite its technological underpinning."

Winners Join the Anti-EVM Chorus

Not just losers, several parties that performed creditably in 2009 polls also joined the anti-EVM chorus. Trinamool Congress which swept Lok Sabha polls in West Bengal, the Janata Dal (United) which swept polls in Bihar and the Congress party in Orissa which registered a nationwide spectacular performance raised concerns about EVMs.

Mamata Banerjee, President of Trinamool Congress party welcomed L.K. Advani's suggestion to revert to the traditional paper ballot system. She recalled that a year earlier, in 2008, when the Trinamool Congress swept the panchayat polls in which ballot papers were used, she had demanded that ballot papers be used in Lok Sabha polls as Electronic Voting Machines (EVMs) can easily be tampered and alleged that the CPM had been rigging the polls through EVMs.

Mamata Banerjee alleged that the strong rooms where EVMs are kept before counting are manned by the state government employees and police. "The CPM is manipulating the machines and reversing the public mandate in Bengal. This year's panchayat elections proved it. Ballot papers are used even in developed

countries. Why can't India revert to ballot papers," said the Trinamool chief then.

Sharad Yadav, President of Janata Dal (United), which swept Lok Sabha polls in Bihar with its alliance partner, the BJP also supported the idea of reviewing the use of EVMs in elections. He said that he had received complaints on malfunctioning of EVMs from the PMK leader S Ramadoss and TDP leader N Chandrababu Naidu and demanded that the poll panel should convene a meeting of various political parties to allay their apprehensions.

Mulayam Singh Yadav, President of the SP demanded that an all-party meeting be called by the Election Commission to quell doubts about the EVMs. SP general secretary, Amar Singh said, "There is a lot of controversy over EVMs in India as well as in the West. *It is found that they can be manipulated. In democracy, perception is very important. If there is doubt among a large section of people, then it has to be addressed".*

Ram Vilas Paswan, President of the Lok Janshakti Party and a cabinet minister in the UPA government for five years lost his own election for the first time from the Hajipur parliamentary constituency. He said his party had encountered complaints against EVMs, ranging from their malfunctioning to their manipulation by the state government and presiding officers. In some cases, officials cast the votes while demonstrating the use of these machines to gullible villagers, he alleged.

Congress Party's Reservations

Like most others, the Congress party also seems to wonder if the EVMs are good or bad for the country. The Congress party is on record alleging that their rival

in Orissa, Biju Jana Dal (BJD) had manipulated elections in that state by resorting to large scale tampering of EVMs.

Earlier, in 2001, Amarinder Singh, former Chief Minister of Punjab and Congress leader criticised EVMs and demanded a roll back to the ballot papers.

How to tamper with voting machines! Demo by Amarinder Singh

March 11, 2001
Tribune News Service

Can electronic voting machines (EVMs) be tampered with?

"Yes", says Mr Amarinder Singh, president, Punjab Pradesh Congress Committee, supporting his assertion by giving a demonstration of how an EVM with a cleverly programmed chip installed in it can transfer votes polled by one candidate to another leaving no remnants of the original voting pattern.

"Convinced that these EVMs can be manipulated..., we are going to request him (Chief Election Commissioner, M.S. Gill) to revert to the original system of voting using ballot papers," asserts Mr Amarinder Singh.

"We got suspicious...The ruling party did well wherever EVMs were used while at other places, we did well. This we did by analysing all elections in the state since 1997," says the PPCC chief.

"Let bygone be bygone. We do not want this 'sophisticated booth-capturing' to continue anymore. We do not want EVMs but want that in all future elections in Punjab the conventional ballot paper should be used.

"The EVMs remain in the custody of the government, thus leaving scope for their manipulation," he added.

Even in the recent assembly elections to the Maharashtra assembly, which the Congress-Nationalist Congress Party (NCP) combine won convincingly, a number of candidates of the Congress and NCP, particularly from Nashik district, have alleged that they lost due to tampering of EVMs by their rival candidates.

Lack of Trust in EVMs

Thanks to the EVMs, the credibility of electoral verdicts has suffered greatly. Parties are looking at EVMs with great suspicion and dread the prospect of EVMs "defeating" them. This mistrust in EVMs is not confined to any single party and is all pervasive.

Today, it is difficult to find parties that vouch for the continued use of EVMs in Indian elections. On the contrary, there is a flood of opposition to the EVMs from the political class.

The political class cutting across all sides of the divide has just one verdict: *We don't trust the EVMs*. This vote of "no confidence" stems from the personal experiences of parties and leaders as well as the nature of results thrown up by the EVMs. The Election Commission was expected to take the concerns of political parties and citizens' groups regarding EVMs seriously and look into possible remedies. Far from it, the hearings of the Election Commission conducted into the matter turned out to be a farce.

8

Farce of Enquiry by Election Commission

The Election Commission of India (ECI) began to "hear" complaints on electronic voting machines after the Supreme Court directed the petitioners of the public interest litigation (PIL) on the EVMs to approach the Election Commission at the first instance. Accordingly, the Commission had invited all complainants including petitioners in different court cases, political leaders and others to demonstrate the points made in their allegations in the Nirvachan Sadan, the headquarters of the Election Commission.

However, the engagement proved to be a futile exercise as the Commission wasn't serious in addressing the concerns of those who had grave doubts about the electronic voting machines and converted the so called "enquiry" into a farce.

The EC had procured about 100 EVMs from around the country and challenged the complainants to tamper with them then and there without opening them.

On the face of it, the challenge thrown at the critics of EVMs seemed fair. But the EVMs – solely manufactured for use in elections – are not available in the open market and no one can demonstrate the tamperability of the machines without being given sufficient access to the EVMs.

How could anyone tamper a voting machine in the commission's custody without opening it, inspecting it and tinkering with it? Perhaps the Election Commission wanted them to display some skills in black magic. Or, the Election Commission expected the criminal-hackers whom I referred to in chapter 5 to come to Nirvachan Sadan and show how they do tampering. That was silly indeed.

To hack an EVM and manipulate its functioning, one has to open the machine and alter the source code (program) in the EVM. For this, the microchip in the EVM has to be replaced with a tampered microchip. Once a tampered microchip is made ready, it would take hardly a few minutes to tamper an EVM. The Commission wouldn't allow any of this.

"The challenge that the Commission posed was not a viable challenge and goes against the fundamental principles of security testing" said Hari Prasad, Managing Director, NetIndia and a "hactivist", when the Election Commissioners asked him to hack the EVMs on August 17, 2009.

Polite to Perfection

The Commission officials seemed to believe that questioning the reliability of EVMs was an attack on the impartiality and integrity of the Election Commission. Possibly due to this reason, Election Commission representatives at these meetings were clearly a worried lot. To overcome this anxiety, the three election commissioners and senior officials were polite to perfection in all the meetings. That was a ploy to win

over the complainants and reduce their virulent opposition to the EVMs.

This strategy had clearly paid off with most of the complainants feeling happy that they had been treated well and they had dominated the discussions. Little did they realise that this was a trap laid out for them to kill their opposition with gestures of phoney kindness. The real attitude of the EC soon became evident.

As soon as the series of "demonstrations" organized between August 3 and 8 finished, the Election Commission issued a press statement claiming, "Today, the Commission once again completely reaffirms its faith in the infallibility of the EVMs. These are fully tamper-proof, as ever."

The press statement issued by the Commission distorted the real nature of conversations that went inside these meetings and failed to even make note of the vulnerabilities of EVMs that were pointed out by the complainants. It became clear that the Election Commission had tricked them; inviting all for a tampering demonstration and not giving them a real opportunity to demonstrate the same.

Many of those who attended meetings with the Election Commission were left seething with anger. Kirit Somaiya, ex-MP, BJP and Omesh Saigal were cut up with the EC's press statement and shot off letters to the Commission objecting to the same. Omesh Saigal asked the Election Commission in an RTI query to supply video tapes of the meeting he attended and the written proceedings of the meeting he attended on August 8.

Quite curiously, the Election Commission refused to furnish the video proceedings of the meeting under the pretext that the "enquiry" was still going on. Election Commission adopted a totally opaque policy with regard to the deliberations and proceedings at meetings that should have been open to public scrutiny.

All the meetings held at the Commission were recorded by video cameras. Some assistants and stenographers were also present at these meetings to record the proceedings.

To give you a glimpse of what happened at these meetings, I have reproduced below a summary of deliberations that took place at the meetings between petitioners in the Supreme Court led by V.V. Rao and the Election Commission representatives on August 17 and September 13 and the correspondence exchanged between them.

August 17, 2009, 4.30 P.M

Nirvachan Sadan

In the meeting held on August 17, petitioners requested the Commission to clarify several concerns regarding the vulnerability of the EVMs raised in their writ petition. After initial introduction and discussions, the following conversation took place in the meeting.

Navin Chawla (Chief Election Commissioner, EC): Instead of wasting time, you should cut short the discussion and demonstrate tamperability of the EVMs.

Hari Prasad (Managing Director, Net India; petitioners): Please put an EVM on the table so that I can practically explain vulnerabilities of EVMs. We would also like to ask some technical questions.

Navin Chawla (impatiently intervenes): I would like you to raise all such questions later in writing. Instead, I want you to demonstrate the tamperability of EVMs.

Hari Prasad: The way you (Election Commission) are asking us to demonstrate is illogical. This is also against the fundamentals of security testing. This is not how ethical hacking is done. We will suggest a procedure for ethical hacking. The manner you want the demonstration done is not viable.

Prof. Indiresan (Technical Expert, Election Commission): I cannot comment on that. You should prove the tamperability of ECI-EVM as suggested by the CEC, Mr. Navin Chawla.

Hari Prasad: We are prepared to give a demonstration. But we have to agree on rules and procedures. Give us a few EVMs and allow us to tamper those using "reverse engineering" technique with the help of necessary tools. Then tell us which of the EVMs have been tampered. If you fail to detect the tampered EVMs, you have to accept that tampering is possible. I am certain that when we tamper them, even the Commission's technical experts cannot detect which machines have been tampered.

Navin Chawla: All right. We would allow you to tamper some EVMs. You can use your tools over many days. But it will be in our premises.

Hari Prasad: We are willing to do the ethical hacking in your premises. We will also suggest a procedure that we propose to adopt for ethical hacking. That will be the basis on which ethical hacking will be done.

Navin Chawla: We welcome any suggestions that can strengthen the security of EVMs. Whatever questions you have, give in writing and the Commission will furnish replies in writing.

Election Commissioners were quite concerned about the technical team led by Hari Prasad as they had seen several demonstrations conducted by them earlier which had shocked the audiences in Delhi, Bhubaneshwar, Chennai, Nagpur and Hyderabad. They were clearly worried that this was one team that had the understanding and capacity to demolish the EC's claims that their EVMs are tamper proof. The EVMs used for such demonstrations were built by NetIndia following the same specifications as that of the ECI-EVMs.

On the sidelines of the meeting, a wary Chief Election Commissioner asked Hari Prasad why they were pursuing the matter so seriously and whether

they really wanted the General Election result overturned.

Following the August 17 meeting, in a letter dated August 28, 2009, the petitioners had submitted to the Election Commission a list of questions concerning the process, design, manufacturing and administration of EVMs and a "Suggested Procedure for demonstration of the tamperability of the Electronic Voting Machines". Petitioners had expected the Election Commission to furnish its response before the next meeting scheduled on September 3.

The procedure suggested for demonstration entailed ECI providing 20 EVMs, a mix of new and old EVMs, used in the elections in different constituencies. Petitioners' team would tamper three or four of these EVMs and then, give all 20 back to the ECI. If the ECI is unable to detect which of these EVMs are tampered, and the petitioners thereafter are able to demonstrate how votes can be switched on the EVMs tampered by them, the Commission should then accept that the demonstration was successful and the tamperability of EVMs has been established.

Anyone would consider that this is a fair challenge. If the manufacturers and technical experts of the Election Commission cannot detect tampering, how on earth would they expect the district officials to detect tampering of EVMs?

But the Election Commission wanted to play safe. Neither did it furnish answers to any of the questions raised by the petitioners, nor did it comment on the procedure for demonstration. Instead, the petitioners were slapped with a legal notice by one of the manufacturers, the Electronics Corporation of India (ECIL) which threatened criminal and civil action against the petitioners for highlighting the vulnerabilities of EVMs through their writ petition in the Supreme Court and in their demonstrations at many

places using a look-alike EVM developed by them. The next meeting on September 3, 2009 took place in the Election Commission against this background.

September 3, 2009, 3.30 P.M

Nirvachan Sadan

Here are some details of how the discussions proceeded on September 3, 2009.

J.P. Prakash, Deputy Election Commissioner (Dy. EC): Let us see the demonstration right away.

Hari Prasad: We have to first define what constitutes tamperability and agree on a demonstration procedure. We have submitted a procedure for demonstration. Without commenting on these, how can we begin to show tamperability? Your approach is illogical and unscientific.

Prof. Indiresan: Demonstrate the tamperability of EVMs at various stages of the electoral process; like polling station Level, Returning Officer level, manufacturer level etc.

J.P. Prakash: As you have alleged tamperability, we would like you to begin demonstration.

Hari Prasad: As you have not agreed on procedure for demonstration, let me begin today inspection of your machines and explain the vulnerabilities at different stages as suggested by Prof. Indiresan.

Prof. Indiresan: I will touch your feet if you tamper the EVMs without replacing the microchips.

This unseemly challenge from the venerable professor surprised the petitioners. Indiresan had made irresponsible and insensitive statements earlier to defend the reliability of EVMs. In a television interview on CNN-IBN, the ageing professor had said, "This (doubting the reliability of EVMs) is like, you know, asking Sita to prove her virginity by having Agni Pariksha." Here he was making yet another wild statement.

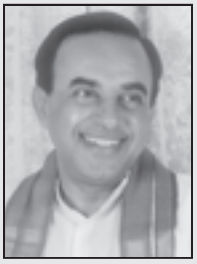
"This is like, you know, asking Sita to prove her virginity (sic) by having Agni Pariksha. That is all I can say"

Subramanian Swamy (Former law minister): (Taking strong objection to Prof. Indiresan's comments) It is a silly comment for you to make. What more can be expected from you? You are an electrical engineer and you know no more than soldering two wires. You are not technically competent to comment on electronic voting systems. To hide your own and EVM's weaknesses, you are making wild statements like "EVMs are as pure as Sita".

Hari Prasad: It is elementary that the program inside the microchip cannot be altered as it is one time programmable. But, in the manner Election Commission conducts its field level checks, there is no way you can find out if a hacker replaces the entire microchip or the mother board inside the control unit of the EVM.

Prof. Indiresan: I agree that it is theoretically possible. But can anyone replace the microchips in all 13.8 Lakh EVMs in the country?

(Indiresan is missing the point. One doesn't have to tamper with all the EVMs to win elections. Elections are won by small margins and even if a few EVMs are managed to alter the votes in one's favour, it can possibly turn a loser into the winner and vice versa.)



"You are not technically competent...to hide your own and EVM's weaknesses, you are making wild statements like "EVMs are pure as Sita".....

J.P. Prakash: Let us start the process of demonstration.

Hari Prasad: Let me begin the process today by inspecting the old and new EVMs used in elections which would be the first stage of demonstration i.e

inspection and analysis. Can you bring a few new and old EVMs to examine and inspect?

J.P. Prakash: Bring whatever EVMs they want to examine.

Hari Prasad: I want these EVMs opened so that we can comment on their vulnerabilities.

There was a sense of unease among the ECIL/ BEL engineers who did not want to open the machines. When Hari Prasad said that no machine can be hacked without opening it, the reluctant BEL engineers were told by the Election Commission officials and Prof. Indiresan to allow the petitioners' technical representatives to examine and inspect the EVMs to make necessary preparations for their tamperability demonstration.

How many votes do you need to flip an election?

Flipping elections doesn't require fixing EVMs on a nationwide scale. Winning or losing elections is decided on small margins.

In 2009 Lok Sabha elections, 164 seats were won by a margin of less than 4 per cent. Of these, 26 were in Uttar Pradesh, 15 each in Andhra Pradesh and Maharastra, Gujarat (13), Tamil Nadu (11), Karnataka (11).

In such marginal constituencies, switching 10,000 votes can turn a runner-up in a Lok Sabha election into the winner.

In case of closely fought assembly contests, switching of a mere 1200 votes would do the trick!

The technical team led by Hari Prasad continued their inspection of the ballot and control units and began to note down the details of card and circuit level checks on plain paper provided by the Election Commission. Hari Prasad and his colleagues looked at each other several times during this process. While noting down the details of the old EVMs, they animatedly discussed the technical flaws and vulnerabilities of the EVMs, which were overheard by the engineers of manufacturers and EC's expert committee members. That was perhaps a tactical mistake they had made as their confidence and the

expressions on their faces showed that tampering these EVMs would be child's play for them.

(After the meeting, they told me that they were indeed surprised that the architecture of the ECI-EVMs is extremely dated and the 'look alike' EVMs that they had built for demonstrations were far superior to the ECI-EVMs. Hari Prasad was emphatic that it did not require their level of skill to hack the ECI-EVMs and even an ordinary technician can tamper with the ECI-EVM's easily.)

As the technical team of petitioners progressed, the BEL Engineers continued to be wary of the inspection being carried out. They suddenly became jittery and rushed to the deputy commissioners and Prof. Indiresan to stall the inspection process lest they be exposed.

J.P. Prakash: Let us stop the inspection of EVMs here.

Hari Prasad: Why?

J.P. Prakash: We need to take the consent of the Election Commissioners before going ahead with the demonstration.

For the first time, since the Election Commission began to dare anyone to demonstrate the tamperability of EVMs, it was clear that the Election Commission and its technical experts had blinked. They appeared to have suddenly lost all their faith in the EVMs which they had claimed to be fully tamper-proof.

J.P. Prakash: (Adopting a conciliatory tone) The Election Commission has an open mind and would welcome any suggestions to improve the EVMs. There is no technology that cannot be improved upon.

Prof. Indiresan: (Betraying a deep sense of anxiety) We want you to submit all your written notes made during the process of inspection.

Jayant Das (Senior Advocate, Supreme Court): On what grounds are you asking us to return the notes? You have invited us for a demonstration and allow us to do it.

Subramanian Swamy: You have been asking everyone, including politicians like me who have written to you over the past two months daring us to demonstrate their vulnerability. Why are you scuttling the process now?

Prof. Indiresan: Give us an indemnification regarding the knowledge that you have gained through the process of inspection that it will not be used for replication.

Jayant Das: (Losing his patience, he asked) Did the officials of the Election Commission of India, members of the Expert Committee and the manufacturers of the EVMs indemnify the people of the country against the misuse of EVMs about which they had exclusive technical knowledge?

Seeing the jitteriness of the EVM manufacturers and the members of the expert committee was a sight to be watched. For the first time, petitioners saw the Election Commission representatives in a totally panicked state. Clearly, the confidence they had exhibited hitherto in the EVMs, thanks to the repeated assurances given to them by the expert committee, had been shaken.

Delay Tactics & Change in Stance

The next opportunity for a discussion and demonstration that the Commission officials had promised to the petitioners did not materialize for over three months despite repeated reminders from the petitioners. In the meanwhile, the Commission went ahead with elections to the state assemblies of Maharashtra, Haryana and Jharkhand using the "old EVMs" which did not meet the improvements suggested by the Indiresan Committee, 2006. Significantly, in the wake of protests from political parties in Tamil Nadu, the Election Commission had stopped use of old EVMs in by-elections held in Tamil Nadu in August, 2009 but had no qualms using the same old EVMs in elections to state assemblies of Maharashtra, Haryana and Jharkhand.

After repeated reminders, the Election Commission wrote a letter to the petitioners on December 14, 2009. The following are excerpts from this communication:

"You may do only normal tampering"

On 31st August, 2009, we received a letter dated 27.8.2009 from you, wherein you suggested some procedures for demonstrating alleged tamperability and also raised a number of technical and procedural questions which you had not raised in your Writ Petition before the Supreme Court...The Commission informed you that the issues raised in your said letter would be examined after obtaining necessary details from the manufacturers and expert committee.

The Commission has now decided to offer you one more chance to demonstrate alleged tamperability of EVMs as available in the field as a final response to your allegations of tamperability of EVMs... *However this has to be restricted to the framework of normal tampering that can happen in the field under security of procedures in place. Any attempt at Reverse Engineering is not acceptable. It violates IP held by the manufacturers of ECI-EVMs.*

The Election Commission's letter of December 14, 2009 acknowledges that the petitioners had suggested procedures for demonstrating tamperability and raised a number of technical and procedural questions in their letter dated 27 August, 2009. Did the Commission not find three and half months (over 100 days) adequate to respond to the questions raised by the petitioners in their writ petition (in Supreme Court) and otherwise? Does this uncooperative attitude on the part of the Election Commission not show that the Supreme Court's trust in this constitutional body is misplaced? If it was serious about the reference made by the Supreme Court, would it take the Commission to clarify issues raised before the Supreme Court over 100 days?

The lack of response of the Commission to the questions raised by the petitioners clearly shows that the Commission had much to hide and had no convincing

explanations to offer to a wide range of questions tha the petitioners had raised ir the Supreme Court anc thereafter.

Another instance of thc Commission's shiftin stance becomes clear from the unrealistic condition the Commission sought tc impose on the petitioners ir proving the tamperability o the EVMs. In their reply the petitioners wrote to thc Commission vide lette dated December 22, 2009:

Comment by an International Expert

Isn't that funny? If research and proper investigation of the equipment is prohibited because it might violate the IP of the manufacturers, a demonstration of vulnerabilities will be impossible. Someone who wants to steal an election is unlikely going to be too concerned about the manufacturers' intellectual property!

Ulrich Wiesner, Successful petitioner in the EVM case in Federal Constitutional Court of Germany

"Arbitrary and unreasonable"

In our August 17th meeting and the meeting held with several other complainants, the Commission had agreed to give full access to your EVMs and that we could work on them for several days, if necessary at the Nirvachan Sadan to demonstrate how they can be tampered with. Going back on this promise, when we inspected the EVMs on September 3 representatives of EVM manufacturers and your technical committee experts appear to have panicked, resulting in a sudden suspension of inspection.

After repeated requests from us, we are now being invited for a demonstration by imposing what on the face of it are arbitrary and unreasonable pre-conditions on the proposed tamperability demonstration. You may kindly note that *hackers of the real world do not work under any such artificially imposed conditions. Then, why impose such conditions on us when we are interested in carrying out an "ethical hacking" operation for promoting the Commission's mandate of holding free and fair elections?*

The above communications between the Commission and the petitioners bring out some glaring facts. First, the Commission refuses to clarify any questions regarding vulnerability of EVMs raised by the petitioners in their writ petition in the Supreme Court. Secondly, the Commission wants a demonstration on tamperability without allowing the petitioners to inspect the machines and hack them as any hacker would do. The Commission simply wanted to impose unrealistic conditions that would make it impossible for the petitioners to show tamperability.

This uncooperative attitude of the commission did not, however, surprise the petitioners. It was precisely for this reason that the petitioners had approached the Supreme Court at the first instance in July, 2009. At the end of January, 2010, the petitioners exasperated with Commission's uncooperative attitude, were contemplating to approach the Supreme Court again.

9

Commission Blocks Ethical Hacking

Contrary to the Election Commission's loud claims that "nobody could hack our EVMs", the Election Commission had thwarted genuine "ethical hacking" attempts at tampering the EVMs by a team of technical experts from NetIndia representing the petitioners in the Supreme Court.

Hackers and Hactivists

The term 'hacker' is used in popular media to describe someone who attempts to break into computer systems. Typically, this kind of hacker is a proficient programmer or an engineer with sufficient technical knowledge to understand the weak points in a security system

But all hackers do not have bad intentions. Many organizations employ 'ethical' hackers to test a security system and use the same methods as their less principled counterparts, to find and fix computer security vulnerabilities instead of taking advantage of them. An

ethical hacker is a computer and network expert who attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious hacker could exploit. Illegal hacking (i.e gaining unauthorized access to computer systems) is a crime, but ethical hacking done at the request of the owner of the targeted system(s) is not.

One such hactivist is Rop Gonggrijp who by his daring demonstration on television at great personal risk exposed the vulnerabilities of EVMs used in Netherlands and this led to instant banning of EVMs in the country.

Rop Gonggrijp is the famed 'hacktivist' from Holland who was instrumental in having EVMs banned in Netherlands. He demonstrated the security vulnerability of EVMs in a live show on national television barely weeks before national elections, leading to the EVM vendor pressing charges against him for 'terrorism'!

His organization *"We do not trust voting machines'* also questioned the inherent lack of transparency when the vote count only happens inside the voting machine. These efforts convinced the Dutch public and government that standalone electronic voting machines are not trustworthy. Holland has since gone back to voting by paper ballots.

Gonggrijp is a key figure in the growing international movement for election transparency and verifiability. He co-authored the technical report on EVMs called for by the Federal Constitutional Court of Germany, on the basis of which the Court went on to ban EVMs in Germany.

He is the founder of the hacker magazine Hack-Tic, and the chief organizer of hacker events held every four years that are attended by thousands of hackers from around the world.

The Election Commission ought to have engaged ethical hackers to understand the vulnerabilities of EVMs. In the event, it should have welcomed ethical hackers who came forward to lay bare its vulnerabilities. On the contrary, the Election Commission did everything possible to sabotage such genuine efforts.

Election Commission Aborts Demonstration

At a tamperability demonstration organized in Nirvachan Sadan, the headquarters of the Election Commission, referred to in chapter 8, the Commission representatives prematurely aborted an ethical hacking effort. This incident took place on September 3, 2009 when the Commission invited the petitioners of the public interest litigation in the Supreme Court to demonstrate vulnerability of EVMs. I was present at this meeting and witnessed these developments personally.

ALLVOICES

Panic stricken Election Commission abruptly halts EVM tampering demonstration

By: Chnarendra
New Delhi : India
September 4, 2009

Going back on its oft repeated assertions that nobody has come forward to demonstrate tampering of the ECI-EVMs, betraying signs of utter panic and nervousness, the Election Commission of India (ECI) has abruptly halted the process of tampering demonstration initiated by the technical experts of the petitioners led by V.V. Rao who filed a writ petition in the Hon'ble Supreme Court earlier. Ironically, the petitioners went to the ECI on a written invitation of the Election Commission to demonstrate Tamperability of EVMs after the Supreme Court has referred the matter to the Election Commission.

A couple of days after the meeting, Hari Prasad, managing director of NetIndia who inspected the EVMs-the first activity in a tamperability demonstration--at the Election Commission on September 3 wrote in the comments sections of the Indian Express:

> By Hari Prasad | Sunday, 6 Sept'09: Surprisingly, we were halted abruptly while identifying the vulnerabilities saying that they (Election Commission representatives) need to take permission from the CEC on our process of tampering. And, yes. We found the EVMs, especially the old ones (9.7 lacs used in this election) appeared so vulnerable to tamper and I can say a Diploma guy can tamper these machines within no time. And, I am sure even the technical committee which has certified these machines noticed us reaching the weak points in these machines and abruptly stopped us to proceed further. Now they said they will give us a fresh date after approval from CEC. Let's hope they stand by it.
>
> http://www.indianexpress.com/comments

Commission Imposes Unreasonable Conditions

Stung by the humbling experience on September 3 when it hurriedly called off the tamperability demonstration, the Election Commission suddenly fell silent and became incommunicado. After several letters and follow up calls, on December 14, 2009, Election Commission wrote to V.V. Rao, the main petitioner in the Supreme Court case on tamperability of EVMs.

The letter made a significant departure from its earlier approach and imposed unrealistic and illogical constraints on the petitioners in conducting the tamperability demonstration. The EC letter said:

> "You are allowed to demonstrate the alleged tampering. However, this has to be restricted to the framework of normal tampering that can happen in

> the field under security of procedures in place. Any attempt at Reverse Engineering is not acceptable. It violates IP held by the manufacturers of ECI-EVMs."

This statement gives away the story. This is in fact a tacit admission that the so called "non-tamperability" of the ECI-EVMs claimed by the Commission is subject to many conditions being met.

Insider Fraud

Election Commission wants to restrict tampering to "normal tampering" that can happen in the field under security of procedures in place. Simply put, the Commission wants to restrict the access of EVMs to the petitioners in conducting a tampering demonstration. Hackers of the real world with a criminal intent do not work under any such "framework of normal tampering".

The big assumption that the Commission makes hear is that hackers cannot gain access to the machines in the field as security procedures are in place. That is bunkum. The biggest threat to the EVMs comes from insiders – the manufacturers, their engineers, engineers hired by them for maintenance and checking of EVMs, microchip suppliers, other vendors and distributors and finally, the district and lower officials etc. – who have access to the machines at different stages in the life cycle or supply their crucial parts.

The Commission wants us to believe that all those handling the EVMs at different stages are angels with unquestionable integrity. The incidents that I have narrated in chapter 5 show that many of these scoundrels involved in this organized crime are insiders having easy access to EVMs. Throughout the world, it has been recognized that the real threat from the electronic voting machines comes from insiders.

A Report prepared by a Commission on Election Reform, co-chaired by the former President of the United States, Jimmy Carter and a former Secretary of

State, James A. Baker III gives a health warning. The Election Commission and the political parties in India would surely benefit from this wisdom.

> The greater threat to most systems comes not from external hackers, but from insiders who have direct access to the machines. Software can be modified maliciously before being installed into individual voting machines. There is no reason to trust insiders in the election industry any more than in other industries, such as gambling, where sophisticated insider fraud has occurred despite extraordinary measures to prevent it. *(Building Confidence in US Elections, Report of the Commission on Federal Election Reform, September 2005, co-chaired by Jimmy Carter and James A. Baker III)*

Prof. David D. Dill, an acknowledged international expert on voting systems also cautions about the potential dangers of an insider job in election fraud. Says he, *"Although many discussions of "hacking" electronic voting systems focus on corruption of the machines by third parties, the greatest threat comes from changes made by someone with legitimate access to the hardware or software design or manufacturing process."* (Rejoinder Affidavit filed by Dr. Subramanian Swamy in the High Court of Delhi in Writ Petition No. 11879 of 2009.)

The above comments by international experts seem to offer an international perspective to the murky developments on the domestic front. In chapter 5, I have referred to "EVM fixing solutions" being offered by insider fixers by quoting staggering sums. While such "insider fixing" concerns have been openly expressed in the United States and elsewhere, in India, we have been sanguine about the role of the EVM manufacturers and their agents, suppliers etc. and have taken their integrity for granted. In a sense, the Indian political parties have not yet fully woken up to the true dangers of electronic voting.

"Reverse Engineering" Not Allowed for Demonstration

One more condition laid down by the Election Commission relates to not permitting use of "reverse engineering" technique for hacking the electronic voting machines. The petitioners found this condition amusing and ironical as the Commission's learned experts had learnt about the possibility of hacking the ECI-EVMs through the "reverse engineering" process from the petitioners in their previous meetings held on August 17 and September 3. In the earlier meetings, the Expert Committee members had contended that 'reverse engineering' was not possible with ECI-EVMs. Amusingly, they were now insisting that "reverse engineering" will not be allowed.

The reason given by the Election Commission for disallowing reverse engineering was that this violates the intellectual property rights of manufacturers. Would any hacker with a criminal intent ever keep in mind the rights of the owners and manufacturers before hacking them?

Commission Changes Demonstration Ground Rules Midway

Earlier, the Chief Election Commissioner himself promised that he would allow the challengers to do everything they needed with the EVMs and for any number of days to demonstrate the tamperability of EVMs. The only condition imposed by him was that such demonstrations should take place in its Nirvachan Sadan premises and he would not allow the EVMs to be taken out. By stalling the demonstration abruptly, the Commission had gone back on this promise.

Excuse of Intellectual Property Rights!

Desperate to see that the demonstration on tamperability fails, the Election Commission has now come up with the feeble logic that the intellectual property rights held by the EVM manufacturers should

not be violated by any demonstration of their tamperability.

It is preposterous for the manufacturers of EVMs to claim the IPR over the EVMs. It is equally so for the Commission to readily and ungrudgingly cede these rights to the manufacturers as the electronic voting machines have been devised and designed by Election Commission in collaboration with the manufacturers. The Election Commission of India website, in its Frequently Asked questions (FAQ's) section says,

> "The EVMs have been devised and designed by Election Commission in collaboration with two Public Sector undertakings viz., Bharat Electronics Ltd., Bangalore and Electronics Corporation of India Ltd., Hyderabad after a series of meetings, test-checking of the prototypes and extensive field trials. The EVMs are now manufactured by the above two undertakings."

The EVMs were jointly developed by the Election Commission and EVM manufacturers. This is what the Election Commission says on its own website. That being the case, how could the Commission surrender intellectual property rights to the manufacturers. It sounds bizarre. Further, the EVMs are in the public domain for performance and conduct of free and fair elections. In such a situation, how could the Election Commission willingly cede its intellectual property rights?

On the face of it, it might have seemed that the Election Commission, a public institution was being guided not by public interest but by obscure interests of the EVM manufacturers. But, perhaps that was not the real motive. The real motive was to use it as a ploy to place hurdles in the path of the petitioners. Being a public body, it could not be seen to be ranged directly against the petitioners. It has thus used the phony plea

of IP rights of EVM manufacturers to block challengers from demonstrating their tamperability. It didn't stop there. The manufacturers even resorted to reprehensible strong arm tactics to stall the challengers in tracks by threatening them with legal action.

Threat of Legal Action

Just days before the scheduled demonstration before the Election Commission on September 3, the Electronics Corporation of India Limited (ECIL) sent a legal notice to all the petitioners in the Supreme Court threatening them with criminal and civil action for demonstrating the tamperability of the EVMs on a look-alike EVM and for alleging that even the ECI-EVMs can be tampered in a similar manner. The legal notice served on the petitioners said:

> My client states that your allegations against the EVM even before the Hon'ble Supreme Court in your affidavits are to be categorized as false statements as you never had an opportunity to experiment on the EVM as the same is not available any where openly in the market. This clearly shows your approach to the Court of Law is only to abuse the process of law.
>
> My client states that you have tried to build a prototype of the EVM manufactured by my client for exhibiting to the public. My client states that except from external look alike you could not make the machine work exactly like the EVM of my client as you do not have the source code...My client states that by building a look alike of my client machine, you have violated the intellectual property rights of my client pertaining to Patent and Design of EVM which are registered with authorities in India.
>
> *(Excerpts from the Legal Notice served on petitioners by ECIL's lawyer)*

The petitioners had earlier demonstrated at different places in the country how the EVMs could be used to

manipulate election results. As the ECI-EVMs are legally not available for hacking purposes, the NetIndia team built its own EVMs, which are similar to the ECI-EVMs in specifications and functionality.

THE HINDU

Monday, Aug 03, 2009

EVMs not foolproof, say technocrats

Staff Reporter

They hold demonstration in a packed IDCOL auditorium to prove their point. - Photo: Lingaraj Panda

RAISING DOUBTS: Members of the Orissa Jana Sammilani giving a demonstration to prove tampering of Electronic Voting Machine in Bhubaneswar on Sunday.

BHUBANESWAR: A group of social activists and technocrats claimed that Electronic Voting Machines (EVMs) were not tamper-proof and demonstrated how desired electoral results could be achieved by manipulation here on Sunday.

An EVM, which was developed by Netindia, an embedded technology-based company from Hyderabad by reportedly meeting all standards and following manuals of Election Commission, was put to test in a packed IDCOL auditorium here.

The demonstration showed an open voting taken in front of politicians, retired bureaucrats and media gave a different result as the machine was tampered with. Orissa was the fifth State where such demonstration on manipulating EVMs was held. The team was going to demonstrate as to how EVMs were vulnerable before Election Commission of India on August 6.

On September 3, at the meeting of the petitioners with the Election Commission, Supreme Court's senior counsel, Jayant Das and Dr. Subramanian Swamy, former Union law minister took serious objection to the legal notice sent to the petitioners by the ECIL, one of the manufacturers of EVMs threatening criminal and civil proceedings for highlighting concerns regarding tamperability of EVMs. These representatives informed the Election Commission that against the background of the invitation extended by the Commission to the petitioners the threat of legal action by one of its EVM suppliers, the ECIL amounted to intimidation of petitioners who were pursuing a cause in public interest.

ECIL's attempts to browbeat the petitioners from going ahead with their plans to expose the tamperability of the EVMs was a sinister attempt to block their tamperability demonstration as the notice was served just a day after the petitioners were invited by the Commission to demonstrate the tamperability of the EVMs.

I have personally attended two meetings held in the Election Commission: one on August 7 accompanying Kirit Somaiya, a former BJP Member of Parliament and Convener of the BJP's cell on EVMs and another on September 3 led by V.V. Rao, main petitioner in the PIL in the Supreme Court.

Both these meetings, each lasting over two hours and my interactions with various other experts clearly brought out one glaring fact: the Election Commission apparently lacks knowledge regarding the technology and various other aspects concerning the EVMs. Through the process of the "EVM" enquiry proceedings, the Election Commission officials, ever ready with the "tamper proof" theory, seem to have had their confidence shaken.

My investigation into the EVMs ran parallel to the Election Commission's farcical enquiry. This probe yielded many insights and revealed many shocking facts about EVMs, which I have summarized in chapters 11 to 13.

10

Voting Machines Demystified

Electronic voting machines used in Indian elections belong to the class of what are called Direct Recording Electronic (DRE) voting machines - as they store the voting data electronically at the press of a button by the voter.

The most crucial aspect involving electronic voting machines is the process involved in registering votes in elections as the integrity of election outcomes depends on the reliability of this simple process.

Balloting Unit

Control Unit

Electronic Voting Machines used in India consist of two independent units, namely, 'Control Unit' and 'Balloting Unit'. These two units are interconnected, when the voting machine is put in operation, by means of a five meter long cable permanently fixed at one end with the balloting unit. The free end is plugged into the Control Unit at the time of operation.

Balloting unit is the unit on which you register your vote inside the voting compartment confidentially. On the balloting unit, there is a provision for display of the ballot paper containing the names of contesting candidates along with the symbols allotted to them. The voter casts his/ her vote by pressing the blue button next to the candidate's name and symbol on the ballot unit.

The vote cast on the Ballot unit then gets transmitted to the Control unit via the interconnecting table and gets stored in the control unit memory. Thus, control unit is the main unit in which all the voting data is stored from where it is accessed on the day of the counting.

Embedded System

In technical terms, the Electronic Voting Machine (EVM) used in Indian elections is a simple embedded computing system designed to perform a few dedicated functions, like recording votes and accessing information like the total number of votes recorded and votes polled in respect of different candidates etc.

The EVM System consists of three hardware sub-systems (balloting unit, control unit and the interconnecting cable) and the software program (or source code) embedded in the microcontroller installed in the control unit. The software dictates the functioning of the control unit and is critical to its proper functioning.

Vote Registration Process

Hardly a few voters who have voted in elections on the electronic voting machines, if any at all, understand the exact process involved in recording of our votes. Except to say that we pressed a button to register our vote on the EVMs, most of the voters, even the most informed and educated, do not know how the EVMs work and record our votes.

When I began to explore the EVMs, I asked the question myself. I could not recall the process accurately myself. I asked many people I know of to see if they could recollect the voting process on the EVMs. It was the same experience with them. Hardly anyone I know of could recall the exact steps involved. Try recalling all the steps yourself. In all probability, you too can't.

In the good old system of paper ballots, we knew exactly how we voted and how our votes were counted. Thanks to the EVMs, we simply trust the voting machines and the election officials to record and count our votes accurately. In exactly a similar situation, the Federal Constitutional Court of Germany held that the use of EVMs is unconstitutional because ordinary voters could not be expected to understand the exact steps involved in recoding of votes on the EVMs.

Now, read the full description of the voting process on electronic voting machines in the Box. It is important that these steps are understood before I take you through the complex technical and legal issues involved in the subsequent chapters.

Voting Process on EVMs

On the day of polling, after the procedural requirements relating to identification of an elector are completed, indelible ink is applied on the elector's forefinger and his/ her signature/ thumb impression is obtained. Then, the elector is allowed to record vote his/ her on the voting machine kept in a separate compartment.

The Presiding Officer/ Polling Officer in-charge of the Control Unit of the voting machine then presses the 'Ballot' button on the Control Unit. This makes the ballot unit(s) ready for recording the vote of the elector and the lamp marked 'Ready' starts glowing green on the ballot unit (s) kept in the voting compartment. This is an indication that the Ballot Unit (s) is now ready to record the vote.

For recording the vote, the elector will have to press the blue button (called the candidate's button) provided on the right hand side of the name and symbol of the candidate of his choice on the ballot unit. For each candidate, a separate blue button is provided against his name and symbol.

When the elector presses the candidate's blue button, the 'Ready' lamp emitting green light on the balloting unit goes off and the corresponding candidate's lamp (LED) provided near his blue button on the ballot unit starts glowing red. Also, a 'beep' sound from the Control Unit is heard by all present, which is a sort of confirmation that the vote has been registered in the Control unit, where all the votes are stored. As soon as the control unit gives the beep sound, Red Light on the balloting unit goes off automatically.

The ballot unit then gets automatically locked and the next vote can be recorded only when the 'Ballot' button on the control unit is pressed again by the presiding officer/ polling officer to allow the next voter to record his vote.

> The process of voting goes on these lines under the supervision of Presiding Officer until the polling is concluded. At the end of the polling process, the Presiding Officer presses the button indicating the closure of recording of the votes in the Control Unit and seals the Unit.

EVMs are Black Boxes

When we vote on electronic voting machines, we are voting into a "Black Box", whose internal working is a mystery to us. We don't know what happens to our vote and in whose favour it gets recorded and counted.

The façade of trust and dependability of the electronic voting machines, in the form of audio visual signals generated by the EVMs, has been designed to give a false sense of confidence to the voters. The gullible voters are led into believing that their votes have been securely delivered to the candidates of their choice.

To elucidate the point, let me draw an analogy from personal computers which most people use today. Ballot Unit on which the vote is recorded is just an input device, similar to a keyboard on a personal computer, while the control unit where the vote is stored is like the Central Processing Unit (CPU) of a personal computer. As in personal computers, the ballot and control units are joined by a cable.

Routinely, we come across many occasions when the CPU fails to receive proper commands or inputs given through the key board due to various reasons. We come to know that such a mistake has occurred as we can see the visual output of our actions on the PC monitor. What if there was no monitor and you just had to give input to the CPU without being able to see the results of your actions? Would you be comfortable just typing into a black box? Certainly not. But, that is what we are made to do when we vote on electronic voting

machines. Electronic voting machines are veritable black boxes. As voters, we have no clue what happens inside them.

Why Voters Don't Suspect EVMs

If the voters cannot be sure that EVMs correctly record their votes, then how come they do not protest their use in elections? There are several reasons for a lack of distrust in the electronic voting machines.

First, the EVMs have been cleverly designed to give the voters a false sense of assurance that their vote has been delivered properly. When a voter casts vote by pressing the candidate key, the LED (red) light next to the candidate button glows instantly and a beep sound emanates from the control unit. These audio visual signs make the voter believe that his/ her vote has been recorded properly. These audio visual signals are illusory and deceptive.

These audio visual signs only indicate that the vote has been recorded in the control unit. Whether the vote has been recorded properly and in favour of the candidate voted for depends on several factors like a) proper linking of ballot and control units, b) interconnecting cable is joined properly between the two units and that c) the software in the voting machine is not tampered with.

Experts of the Election Commission admit this. *"The data is transferred from Balloting unit to the control unit through the Interconnecting Cable. The faithful recording of the voting data, unbiased and tamper proof functioning of Control unit is critical to the conduct of a fair election,"* observed the Report of the Expert Committee (2006) of the Election Commission.

Unaware of this aspect, voters feel secure when the red light glows next to their chosen candidate (and a beep sound is heard). Voters get hassled only when the red light does not glow properly. The reality is that an

apparently robust EVM may exhibit audio visual signs correctly even when it has been tampered with. A large number of cases cited in chapter 4 would not have occurred if this was not the case.

Secondly, the voters' distrust of polling officials is so high that gullible voters naively believe that officials cannot manipulate votes cast on sophisticated machines. Thirdly, voters are mystified and bamboozled by technology and tend to trust it implicitly.

EVM Manufacturers

The Indian EVMs have been devised and designed by Election Commission in collaboration with two central Public Sector undertakings viz., Bharat Electronics Ltd., Bangalore and Electronics Corporation of India Ltd., Hyderabad keeping mostly intact the salient features of the earlier system in which ballot paper and ballot boxes were used. All the EVMs used in Indian Elections are manufactured by these two central PSUs.

Whenever anyone raises questions regarding the security of the EVMs, the Election Commission is quick to cite this fact. A press release issued by the Election Commission dated August 8, 2009 said; "ECI-EVMs are manufactured only by Electronics Corporation of India Limited (under the Department of Atomic Energy) and Bharat Electronics Limited (Ministry of Defence), both Central Public Sector Undertakings, which are entrusted with development of very high security product/ equipment development."

Both these companies are 100 per cent government owned and government controlled companies. The Election Commission of India has no administrative control over these public sector companies, whatsoever. CPI (M) General Secretary, Prakash Karat told the Election Commissioners in a meeting on September 7, 2009, "Election Commission must get the manufacture of the EVMs directly under its supervision and control."

Omesh Saigal, a retired senior IAS officer wrote to the Commission on June 30, 2009 expressing reservations on similar lines saying, "The fact that the BEL and the ECIL are 100% government owned and controlled does not in the least alter the position (offer any protection): in fact, it makes it worse. The Venezuela election of 2004 is under a cloud merely for the fact that the voting machines were made by Bizta, a company in which government had 28% shares."

Types of EVMs

There are two types of EVMs that are being currently used: old EVMs and new EVMs. Old EVMs are those manufactured before 2006 and lack certain security features. Upgraded EVMs manufactured after 2006 have security features like dynamic coding of Key numbers to enhance the security of data transmitted from Ballot Unit to Control Unit and 'date-time stamping' that records the time and date of every key pressed on the EVM in its memory.

The Expert Committee of the Election Commission headed by Prof. P.V. Indiresan in 2006 recommended that EVMs be upgraded for their tamper proof working.

Use of Upgraded EVMs Recommended

The Committee stated, "...the committee to the best of its ability has looked into all possibilities of tampering with the EVM and has come to the conclusion that there is no way of altering the results of the polls before, during and after the poll duration provided, due security precautions already in force and additional modifications suggested by the committee are enforced and the sealing at various stages is adhered to."

It further added, "In view of all these factors, the Committee unanimously certifies that the EVM system is tamper-proof in the intended environment when due precautions are taken. For these reasons, the Committee

recommends that the upgraded EVM with suggested modifications, testing and operating precautions may be accepted and put to use."

In the above two points, it is noteworthy to mention that the Committee had emphasized that the EVMs will be tamper proof only if additional security precautions are enforced and the EVMs are upgraded with the suggested modifications, testing and operating precautions.

Disregarding the recommendations of its own Expert Committee, the Election Commission has extensively used old EVMs in the recently concluded Lok Sabha and assembly elections.

Upgraded EVMs

Following the recommendations of the Committee, ECI-EVMs were upgraded or manufactured anew incorporating suggestions made by the Expert Committee. However, these are only 'relatively' tamper proof.

The expression 'relatively' tamper proof is being used here as the Committee had overlooked some key security aspects of the EVMs. For instance, it failed to ensure that a software and hardware audit is carried out on every EVM before its use in elections (with the help of an "Authentication Unit") and instead, approved the idea of conducting functionality tests which are superficial and cannot detect tampering of EVMs. Further, it failed to recommend use of more secure microcontrollers rather than easily swappable 'generic' microcontrollers used by the manufacturers.

Nonetheless, the upgraded EVMs offer a better level of security with provisions like dynamic coding of Key numbers to enhance the security of data transmitted from Ballot Unit to Control Unit and 'date-time stamping' that records every key pressed on the EVM in its

memory. Given these provisions, while tampering of the improved EVMs is also possible, as in the case of old EVMs, a post election audit is likely to expose the fraudulent attempts as all keys pressed are recorded in its memory.

11

EVM Software isn't Safe...

If there is one thing that can make the EVMs prone to tampering, it is undoubtedly the source code (commonly referred to as software program) in the EVMs. Source code is critical to the functioning of an EVM and controls all the operations of the control unit of EVMs where the voting data is stored. The electronic voting machines are safe and secure only if the source code used in the EVMs is genuine and is not tampered with.

Source Code

Source code is a collection of statements written in a human-readable computer programming language that helps the EVMs to perform a set of dedicated functions and computing tasks. The hex/ binary code generated from the source code is "fused" onto the microcontrollers (commonly referred to as computer chips) installed in the control units of the EVMs.

Therefore, to ensure that the election results are not manipulated by unscrupulous individuals, the source code in the microcontrollers must remain unaltered.

The following observation made in the Report of the Expert Committee on EVMs appointed by the Election Commission (2006) corroborates this view;

> "If the integrity of original program in the microchip is maintained...., then the election through (the) EVM will be fair."

The Election Commission claims that it has taken many steps to ensure that the source code is properly protected. Each of these steps is riddled with serious shortcomings and gaping security holes.

"Secrecy" of the Source Code

The Election Commission says that the source code is highly protected and no one has access to it, except the high ranking officials of the two manufacturing PSUs namely, the Bharat Electronics Limited (BEL), Bangalore and the Electronics Corporation of India Limited (ECIL), Hyderabad.

This is untrue. There are many others who have access to the source code other than the above individuals. One such group is the programmers who have developed the source code used in the EVMs. While some of them may be working with the manufacturers, others may have left.

The Election Commission thinks that the 'secret' programming code in the hands of central PSUs and known to a select few will remain with them and not be disclosed to anyone even in the government.

A famous Spanish proverb reads, *"A secret between two is God's secret, between three is all men's."* This couldn't be truer if the 'secret' happens to be a piece of vital information concerning such a sensitive process as elections.

Can we smugly assume that the source code available with a few persons would remain a heavily

guarded secret? Certainly not. In chapter 5, I have cited specific instances of some purportedly "authorised" engineers of EVM manufacturers going around striking deals with candidates for fancy amounts for "fixing" elections. Against this background, making an assumption that the source code of EVMs is completely secure is utterly ridiculous and dangerous.

The Election Commission repeatedly avers that we have to trust the PSUs because they are government owned and supply highly sensitive defence equipment. But, knowing how generally the central public sector organizations function in India, is it possible for them to deny access to the source code if some higher up in the echelons of government were to demand it?

Not convinced? Come on, if some central PSUs can make donations to the ruling party for fighting elections, is it unreasonable to assume that they would reveal the source code used in the EVMs to those in charge of their administrative ministries?

BJP questions donations to Congress by PSUs

New Delhi, Oct 26 (PTI) Strongly objecting to two public sector firms paying political donations to the Congress party, BJP today said this violated all propriety and demanded action against the guilty.

"The Congress and the two public sector companies MMTC and STC, whose names have figured in reports, should clarify their stand on this issue," senior BJP leader Arun Jaitley said.

He said the details of these donations, which were reportedly obtained through an RTI application, should be furnished to the Income Tax Department and the Election Commission as well.

"The question is not what amount was involved but what it means if public sector companies start giving donations. We would like a clarification from them (Congress and the PSUs)," he added.

Unraveling the Source Code

Even if we (unrealistically) assume that the 'secret' source code known to a select few is completely secure and a leakage has not occurred, a determined hacker can unravel the software with some effort. Curious, how that is possible?

A team of American scientists from the University of California have shown how hackers can 'steal' ballots from Electronic Voting Machines using a 'reverse engineering' technique even if they had no access to the source code or any other proprietary information.

Computer Scientists Take Over Electronic Voting Machine with New Programming Technique

Science Daily (Aug. 11, 2009) - Computer scientists demonstrated that criminals could hack an electronic voting machine and steal votes using a malicious programming approach that had not been invented when the voting machine was designed.

"Voting machines must remain secure throughout their entire service lifetime, and this study demonstrates how a relatively new (return-oriented programming) technique can be used to take control of a voting machine that was designed to resist takeover, said Hovav Shacham, a professor of computer science at UC San Diego's Jacobs School of Engineering and an author on the new study presented on August 10, 2009 at the 2009 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections (EVT/WOTE 2009), the premier academic forum for voting security research.

The computer scientists had no access to the machine's source code-or any other proprietary information-when designing the demonstration attack.

"Based on our understanding of security and computer technology, it looks like paper-based elections are the way to go...These kinds of paper-based systems are amenable to statistical audits, which is something the election security research community is shifting to," said Shacham. "If you are using electronic voting machines, you need to have a separate paper record at the very least."

"This work shows how difficult it is to design voting machines that will remain secure over time. It's impossible to anticipate what new kinds of attacks will be discovered in the future," said Halderman.

Source: http://www.sciencedaily.com

The U.S. demonstration has revealed that reverse engineering technique can be used to unravel the 'secret' source code. For this, a hacker needs to gain access to an EVM to make different kinds of attacks on it–invasive, semi-invasive and non-invasive to unravel the source code. Once the code is cracked, a hacker can build duplicates in a jiffy.

Risk Factors

According to the Election Commission, the source code in the EVMs cannot be tampered as the software program is fused permanently into the microcontrollers. The Report of the Expert Committee (2006) mentioned,

> "The program is burnt into the microchip on a "one time programmable" basis (OTP) and once burnt it cannot be read, copied out, altered and re-fed into the chip at all. It can be fed once only in the chip, and that too only at manufacturing level, is secret and not amenable to any changes once installed in the machine."

On the face of it, it appears like a good protection against tampering of the EVMs. But, in implementing this measure to apparently safeguard the EVMs, the Election Commission and the EVM manufacturers have exposed EVMs to the following grave risk factors.

Risk Factor 1: "Secret" Software given to Foreign Companies

The microcontrollers (chips) used in the ECI-EVMs are sourced from manufacturers in the United States of America and Japan through their vendors in the country. The microcontrollers used by Bharat Electronics Limited (BEL) are manufactured by M/s Microchip, USA, while the Electronics Corporation of India (ECIL) uses microcontrollers from Microchip and Renesas, Japan.

There is no security *concern per se* in procuring microcontrollers from foreign manufacturers as this is merely a piece of hardware. After procuring the microcontrollers from these manufacturers, the EVM manufacturers, namely the BEL and ECIL, could have fused program in the microcontrollers, as "One Time Programmable - Read Only Memory (OTP-ROM)" chips, in their own manufacturing premises. This would have ensured that the program in the microchips remained secure.

But, what these manufacturers have done shocks your senses. They have shared the 'top secret' software program with these chip manufacturers so that they can fuse the source code permanently into the microcontrollers at the time of the manufacturing process itself as either OTP-ROM' (in case of BEL) or 'masked' chips (in case of the ECIL).

This means, the Source Code used in Indian EVMs had been made available to the foreign companies manufacturing microcontrollers. When the microcontrollers fused with source code are delivered to the EVM manufacturers, the EVM manufacturers cannot read back their contents as they are either OTPROM or masked chips. In other words, if the source code in the microchips is tampered or inserted with malicious programming, the EVM manufacturers cannot detect it. Can there be anything more atrocious than this? This is a huge flaw in the Indian EVMs and puts Indian elections at the gravest risk.

Strangely enough, the Election Commission does not have access to the source code used in the EVMs which has been shared with the foreign manufacturers. I wonder if the Election Commission and the EVM manufacturers reckon that the best way to keep the "top secret" source code secure is by sharing it with foreign manufacturers!!

Asked to explain, the Election Commission does not

have any convincing answers and cites disingenuous responses like the following in support of its actions.

> "...machine code of the source (programme) code known as hex-code (not the source code itself) is given to the microcontroller manufacturers for fusing in the micro controllers. From this machine code, the source code cannot be read. Source code is never handed over to anyone outside the software group." (Press release of Election Commission dated August 8, 2009)

The Commission's above formulation that the "source code cannot be read from hex code" is bunkum and a clever fabrication. Any Basic Level Embedded programmer can decipher the source code from the Hex code.

The decision of the EVM manufacturers to get the chips 'fused' by the chip manufacturers located abroad, rather than in their own manufacturing premises in India, which is very much possible, is inexplicable. While the chip manufacturers may be large, reputed multinational companies, should the EVM manufacturers not have done this sensitive operation more securely in their own premises rather than in a third location outside the country?

Involving foreign companies willy-nilly involves the services of many others. This includes local (India based) vendors / distributors of foreign companies and other intermediaries like courier or custom clearing agents in sending the source code to them and in receiving and delivering the microcontrollers to the EVM manufacturers after they are fused.

Election Commission says that questions and doubts on integrity could have been raised on the process even if the source code was 'fused' onto the chips at the manufacturer's premises. That argument is fallacious. The ECIL and BEL, being public sector manufacturers

in India, can be held accountable for their actions, if anything was found amiss. What accountability and control does one have over foreign manufacturing companies involved in such a critical process?

Several doubts and questions arise and must be answered by the Election Commission. Who was responsible for taking these decisions that necessitated revealing the 'secret' software code to the foreign manufacturers? Were these decisions taken by the manufacturers independently or were they made at the behest of the Election Commission or the Government of India? And, what were the compelling reasons for making this decision?

So far, the Commission has evaded answers to all such vital questions. Though the present commissioners may not have been around at the time when these decisions were taken, it is nevertheless important that the Election Commission answers these questions, however inconvenient, as they have serious security implications.

Risk Factor 2: Software Not Checked by Anyone

What if the microcontrollers supplied to the EVM manufacturers contain some malicious programming, apart from the original source code when they are delivered through multiple local vendors and other intermediaries? To rule out such a possibility, when the microchips with fused program code are delivered to the EVM manufacturers, one would expect them to verify whether the program in the chips is the same as what they have supplied to the foreign manufacturers or has it been tampered with.

Shockingly, neither the EVM manufacturers nor the Election Commission check whether the software fused in the microchips is original or not. They just carry out some functionality tests to establish that the EVM is functioning properly. If the EVM is functioning properly,

they would conclude that the source code is secure. This is a highly unreliable method and exposes the EVMs to serious security hazards. Even if a Trojan (Refer Box) is introduced in the original program, the EVM manufacturers cannot detect its presence as they are not checking the originality of the software.

Trojan is a malicious program that can manipulate election results when inserted in the microchip of the EVMs along with the original source code. A significant feature of Trojan is that it disappears after it performs its destructive act. It does not leave any traces and cannot be detected even if a post-poll investigation is carried out. *This is a sort of robbery that can only be prevented if you have the necessary safeguards, but cannot even be established through any post-poll audit or verification. That is what makes Trojan deadly and dangerous.*

Trojan Horse

Trojan Horse or Trojan in short is malicious programming that can manipulate election results when inserted in the microchip of the EVMs along with the original source code. Trojan sits silently in the original software of an embedded system and can gain control of the system and do its chosen form of damage once activated. The activation of Trojan can be done by a hacker by pressing a sequence of keys on the keypad of the system.

If the original microchip in the EVMs is replaced with one having Trojan --at any stage of the life cycle of an EVM beginning with its manufacture until its use in elections-it becomes vulnerable to manipulation.

A key feature of the Trojan is that it goes undetected in routine functional testing and can be detected only in case a software audit is carried out. Thus, the present testing procedures adopted by the Election Commission and the manufacturers that involve only functional testing cannot detect the presence of Trojan in microchips, if any.

As a result, the EVMs that contain Trojan will continue to function normally even after the Trojan is activated if it is cleverly programmed. For instance, the Trojan may be programmed such that it starts manipulating results only after a certain number of votes are polled, say 200 votes. As the number of votes polled in the functionality based 'mock' tests is always much less in number, the Trojan will remain undetected in such cases.

Even the Election Commission does not carry out proper checks. In a RTI reply, the ECI says:

"The Commission has not conducted any software check at the time of delivery of the EVMs. ECIL and BEL have been asked to deliver EVMs directly to states. At the time of receiving the EVMs by the Chief Electoral Officers/ District Election Officers in the states, its functioning is certified by them. However, functionality test is conducted on the EVMs to ensure that they function as per the requirements."

The Election Commission's confession is indeed frightening. It means that neither the EVM manufacturers--ECIL and BEL-nor the Election Commission at any stage of manufacture, delivery or use of the EVMs undertake any check to see if the program in the EVM is original or tampered.

Risk Factor 3: Manufacturer Also the Certifying Authority

As if ensuring the integrity of elections was just a formality, the Expert Committee had suggested that the Election Commission should obtain a 'certificate' from the manufacturers "to ensure that they (the EVMs) are working satisfactorily and according to the original embedded program."

Prescribed certification presently involves checking all the switches of the control and ballot units and testing whether the EVM is working properly by polling 10 dummy votes. The originality of the embedded

program (or source code)-which is the most vital aspect to ensure fair election--is not checked. Thus, this "certificate" offers no protection whatsoever against the tampering of EVMs.

Certification process is inadequate for another reason. Asks Omesh Saigal, what purpose would it serve if the manufacturers of the EVMs also certify their authenticity? In his letter to the Election Commission, Omesh Saigal wrote:

> "If as it seems, the EC is relying on the certificate given by the manufacturer, we have no protection whatsoever against the manufacturer itself preparing a programme (with Trojan horse) and fusing it into the chip/ circuit board."

Is there a way to ensure that these fears are unfounded? Yes, says Saigal. In his letter to the Election Commission, Saigal has offered the following suggestion:

> "....these safeguards are mere cosmetics; what we really need is a fool-proof method of checking whether the software in any/all machines has been corrupted through lapse of time or deliberate tampering or was so corrupted in the first place. For this pre-elections check and post-election audit, covering specifically its software related items, is a must."

Open Source Software

In computer parlance, 'open source' refers to software code that is publicly available for inspection by any one interested. The source code used in the EVMs is kept secret and hence is not available in public domain. Making the software in the EVMs open source would have allowed parties and candidates to use what are called verification tools to satisfy for themselves whether the EVMs contain the original software or a tampered code.

Computer and network security expert, Vijay Mukhi believes that the best way to enhance the security of the EVMs used in elections is by making public the software on which the EVMs operate. Interestingly, policy guidelines of the Government of India stipulate that all systems used for e-Governance including Government to public systems must conform to the standards based on the Open Standards Policy of the government.

Elections are an integral part of the processes of democratic governance and thus Electronic Voting Machines used in elections are a part of digital governance. That being the case, not following open standards in EVMs is in violation of the UPA government's stated e-governance policy.

Ensuring the integrity of the source code in the EVMs is vital to ensuring a "fair" election. It is the duty of the Commission to ensure that the source code's integrity is maintained in the EVMs to ensure free and fair polls.

For ensuring fair elections through EVMs, the Election Commission was expected to take proactive steps to understand their technical vulnerabilities and find ways to fix security loopholes. The Election Commission did exactly the opposite: to block genuine attempts in highlighting such vulnerabilities.

"Back Doors" to Manipulation

Hiding functions in software programme is called putting in "back doors". Visit any computer forum on the internet and you'll find the programmers can think up back doors faster than anyone can figure out how to test for them. I spoke with sources who had worked for voting-machine companies and who came up with one method after the next. Here are some of their ideas:

- Create a program that checks the computer's date and time function, activating when the election is scheduled to begin, doing its work, and then self-

destructing when the election is over. It is possible to write hit- and-run code that changes the original votes, then destroys itself. It can pass testing because it activates only on Election Day.

- Create a dummy ballot using a special configuration of "votes" that launches a program when put through the machine. Quite diabolical, actually: You rig the election by casting a vote! You could extend this to all machines using the same software by embedding the program in the "ender card", which is run through some systems to close the election.
- Create a replacement set of votes, embed them on a chip, and arrange for someone with access to substitute the chip after the election. Chip replacement took place in the 2002 general election in Scurry Country., Texas. Another chip replacement was done in 2002, also by ES&S, in south Dakota, where technicians discovered a machine double- counting Republican votes.
- Add a field into the program that attaches a multiplier to each vote, based on party affiliation, rounding one party slightly up and the other slightly down, using a decimal so that when votes are printed one by one (which is almost never done), they round off and print correctly, but when tallied, the total is shaved. For example: "Affiliation = Democrat; multiplier = 0.95 ... Affiliation = Republican; multiplier = 1.05". This will create totals that correlate with demographics.
- Buy a tech and plant him as a poll worker in a key precinct where your competitor's machines are used. Have him go through the training and then have him flub the election by preventing machines from booting up, or causing them to crash and then blaming it on the manufacturer. If things really get messed up, have him call the press and grant interviews.
- Using wireless technology embedded in the voting machine, monitor the election results on a remote basis as the contest proceeds and send your adjustment in when the election nears its end.

- Put a backdoor into the compiler used for the source code (a compiler is used to "compile" software code from a high-level programming language into faster machine language). The source code can be clean, but no one looks at the compiler and with this method, the digital signature (a method for detecting changes in software after certification) will remain intact.
- Compromise the binary code, below the level of the source code, which will not be detectable even with a line-by-line examination of the source code and won't be solved by using a digital signature.

  By the way, almost everyone who works on computers knows that strong magnets and magnetic storage don't mix.

Bev Harris, Black Box Voting

12

.....Nor is Hardware

In the previous chapter, we have seen how the software installed in the EVMs is not safe. Let me now give you the bad news. Even the hardware in the EVMs is not safe.

Microcontrollers Can Be Faked

Electronic voting machines have a very important piece of hardware called microcontrollers. Microcontrollers are the chips onto which the software (source code) of the EVMs is fused (copied).

A *microcontroller* is a small computer on a single integrated circuit. Unlike microprocessors used in personal computers, microprocessors used in EVMs are designed to perform only small and dedicated applications. Such microcontrollers are extensively used as embedded systems in office machines, appliances, power tools, and toys etc.

The manufacturers of EVMs, both ECIL and BEL, use 8 bit generic microcontrollers. *The same 'generic' microcontrollers are also used in appliances like washing machines, electricity meters etc. They barely cost about*

Rs.100 each and can easily be procured from vendors located in any part of the world. It would take you all of five minutes of Google search on the internet to locate vendors having ready stock of these microcontrollers and place an online order with them. That is how easy it is to 'legally' procure the same make and model of microcontrollers used in the Indian EVMs.

Once you have managed to get the same make and model of microcontrollers, all that you need is to fuse malicious software onto them to perform the same dedicated functions in the manner you want. In the previous chapter, I have described how the "secret" software may not be that secret after all. Once the 'fake' microchips are readied, the hacker needs access to the electronic voting machine to replace the original chip with the fake one. This would take no more than a couple of minutes. And with a de-soldering machine, it can be done in a matter of seconds.

Once this has been successfully done, no one would be able to figure out the fraud as nobody checks either the originality of the microchip or the software at any stage after the EVM leaves the factory. This is so as neither the Election Commission nor the manufacturers have undertaken any hardware or software audit till date.

Gaining access to the electronic voting machine is the key to this operation. In chapter 13, I have dealt with the lax storage of the EVMs. So, hacking of the EVM could happen months before the elections. If these are state government owned machines, even before they are supplied for the conduct of assembly and Lok Sabha polls, they may have been "fixed".

'Generic' Microcontrollers Not Secure

The Election Commission and the EVM manufacturers have made hacking of very easy by using 'generic' microcontrollers, rather than using what are

referred to as Application Specific Integrated Circuit (ASIC) microcontrollers or Field Programmable Gate Arrays (FPGAs).

Unlike generic microcontrollers, ASIC microcontrollers are customized for a specific use and for a specific customer and are not sold to any other customers by the chip manufacturers. As a result, the ASIC chips are far more secure as the entire source code is converted into a specific hardware and the chip is so designed that it can function only for the purpose of the original customer.

A Field Programmable Gate Array (FPGA) is an integrated circuit designed to be configured by the customer or designer after manufacturing-hence "field-programmable". The ability to update the functionality after shipping, and the low non-recurring engineering costs offer advantages for many applications.

Given the sensitivity and importance of the voting machines, the manufacturers should have used ASIC chips or FPGAs, which are custom built and cannot be procured by any unauthorised person as they are not available in the market.

Easy availability of 'generic' chips used in the EVMs renders the ECI-EVMs vulnerable to tampering. Not taking this elementary care has endangered the security of the ECI-EVMs. Repeated queries to the Election Commission in this regard failed to elicit any response.

Cost could not have been a factor in this decision as the ASIC chips or FPGAs, with a large volume of the order as required by EVM manufacturers, might have actually proved to be cheaper and a far more secure option.

Replacement of Mother Boards/Cards

Not just the microcontroller, a hacker can even replace the entire mother board of the Control Unit of the EVM which contains the microchip. Replacement

of a mother board with a tampered chip is much easier and can be done in a matter of three minutes and by a junior technician of the type you would find in every electronics or mobile repair shop. The mother boards in the EVMs are snap fit and can be removed at a click.

The Election Commission appointed Expert Committee's report of 2006 recognized this possibility: it said

> "For introducing a (tampered Trojan horse) programme, considering the nature of production technology of the Control Unit (CU), Ballot Unit (BU) electronic cards, the only possible process is to "physically replace" the CU card by another one containing a tainted micro-chip..."

This is a major security flaw in the design of the ECI-EVMs. The EVM would continue to function normally even if the original microchip (or the mother board as a whole) is replaced with a tampered chip.

Replacement of EEPROMs

EEPROM (Electrically Erasable and Programmable Read Only Memory) is where the voting data is stored inside an EVM. There are 2 EEPROMs inside each Control Unit. Two EEPROMs have been provided for to facilitate conduct of two elections, say Lok Sabha and assembly, simultaneously on the same EVM. But, the Election Commission has never used the same EVM to conduct simultaneous elections to parliament and assembly.

The Control Unit has two result buttons: Result 1 and Result 2. If the Result 1 button is pressed, the control unit will read data from the first EEPROM to which it is connected and if the Result 2 button is pressed, if will read the data from the second EEPROM.

As the EVMs are being used to conduct only one election at a time, the second EEPROM is redundant.

The voting data in the first EEPROM is perhaps also being mapped into the second EEPROM as a back up. But, reports of 'lost' ballots from several polling stations (cited in chapter 4) show that this may not be the case.

Shockingly, these EEPROM's are also generic chips and are unsecured. Any junior programmer can map and manipulate the memory inside these EEPROMs using the instruction set which is available from its datasheet that's open anywhere on the web.

For creative external and internal hackers, the possibilities, it appears, are endless.

Display Unit is Unprotected

Control units have a display unit to display the results of the election. Display unit is fixed with a wire to the control unit. It is completely unsecured. If a hacker replaces the original display unit with one having a tampered chip or inserts a chip inside the original display unit, it can help you manipulate election results very easily. This is a simple way to alter election results without tinkering with the original embedded program in the OTP-ROM or masked chip nor interfering with the ballot unit or the polling process. This gets activated only at the counting stage and no one would be able to detect it. (Details of the same are furnished in chapter 11 under the sub heading: Easy ways to Hack Indian EVMs: After Elections)

Replacement of the EVMs as a Whole

If you thought all the above cases of replacing different "parts" of an EVM are simple, here goes an even better one: the EVMs can be replaced as a whole.

The EVMs developed by BEL and ECIL--both the old EVMs and the new EVMs-are not "replication proof". This is a serious security flaw in the EVMs.

This means that if the original EVMs are replaced by another set of imitation EVMs based on the same

design and functionality but with tampered software, they will go undetected. Yes, that is true. But this is a large scale, mega fraud and requires the complicity of insiders.

To detect such fraud, the upgraded EVMs have a provision to interface with an Authentication Unit that would allow the manufacturers to verify whether the EVM being used in the election is the same that they have supplied to the Election Commission. The Expert Committee of the Election Commission, in its 2006 report on the upgraded EVMs asked the manufacturers to certify after undertaking the "self test signature of the machine" that the EVMs used in elections are original machines. The Committee said:

> .....as a preventive measure, the Committee recommends that before every election the manufacturers may be asked to check (this can be done very fast through a very simple exerciser) and ensure that all the units are functioning as designed. Incidentally, this method will be checked, by what is called the self test signature of Machine and thereby the Manufacturers will be able to certify that the Machine is identical to what they has supplied and it has not been modified or replaced by any other.

As per this plan, an "Authentication Unit" was developed and tested but the project was mysteriously shelved at the instance of the Election Commission or the same Expert Committee that suggested it earlier. Sounds very strange, right? Details concerning the scrapped Authentication Unit project are given in chapter 2.

EC is Clueless on Technology

The Election Commission has adopted the EVM technology about which it has practically no knowledge. Government functionaries involved in the conduct of

Elections at the state and district levels also do not have a proper understanding of the vulnerabilities of EVMs. They even find it difficult to operate the EVMs independently.

In the traditional paper ballot system, the Election Commission had complete control over the entire election process. All the functionaries engaged in the election process were under the control of the Election Commission.

The Representation of the People Act, 1950 (Section 13 CC) which comprehensively deals with all issues concerning elections to the House of People and Legislatures of States says,

> "The officers (Chief Electoral Officers, District Election Officers, etc.) referred to in this Part and any other officer or staff employed in connection with the preparation, revision and correction of the electoral rolls for, and the conduct of, all elections shall be deemed to be on deputation to the Election Commission for the period during which they are so employed and such officers and staff shall, during that period, be subject to the control, superintendence and discipline of the Election Commission."

Under the present electronic voting system, because of its lack of technical knowledge, the Election Commission has delegated a number of crucial functions and technical aspects regarding the conduct of elections – like manufacturing, checking and maintenance of EVMs – to the public sector EVM manufacturers, the ECIL and BEL. But the Election Commission has no administrative control over these public sector manufacturers and their "authorised" agents and representatives engaged in election duty.

None of the election commissioners, neither the present commissioners nor their predecessors, have

proper understanding of the EVM technology. Though the Commission has many young, impressive and competent deputy election commissioners – this is what I had realized when I met them during the meetings at the Commission – none of them seem to have a technical background and a proper understanding of the vulnerabilities of EVMs.

The only source of technical understanding for the Election Commission is a Committee of technical experts, which it set up in December 2005 under chairmanship of Prof. P.V. Indiresan, with Prof. D.T. Sahani & Prof. A.K. Agarwala of IIT Delhi as members.

For reasons best known to the Commission, it has ignored many recommendations of its Expert Committee to make them more secure. Even the Expert Committee is itself unaware of numerous hacking possibilities that I have documented in this book. With such severe limitations, the Commission is not in a position to prevent "electronic" fraud.

"Insider" Fraud

Insider fraud has endless possibilities as the district officials, "authorised" technicians of EVM manufacturers and others in the chain of custody of EVMs have free access to the EVMs.

Unlike in the traditional ballot system where only the election officials were the "insiders", electronic voting machine regime has spawned a long chain of insiders, all of whom are outside the ambit and control of the Election Commission of India. This includes the employees of the manufacturers of EVMs – BEL and ECIL (both are wholly government owned central public sector undertakings) – private agencies or outsourcing agents supplying 'authorised' engineers for checking EVMs (some of them allegedly with political connections), foreign suppliers of microchips, their vendors, carrying agents etc. etc.

All the above agencies are a source of potential hazard and the Electon Commission has no control over them, whatsoever.

There is every possibility that some of these "insiders" are involved in murky activities in "EVM fixing" elections. Personal accounts from well placed sources and experts that some "insiders" are offering EVM fixing solutions only confirm these apprehensions. I have referred to such cases in chapter 5.

Weak Links in Human Chain

You have to trust your elections official, but that's not all. The weakest link in the human chain can destroy the integrity of the election simply by swapping a memory card or popping in a USB memory stick. The human chain includes the programmers at the company that manufactures the voting machine; the subcontractors who maintain and service the machines; each person who has access to the voting machine warehouse (which may include the janitor, the sheriff, and the transportation crew); employees of the elections division; and the designated elections administrator.

Those in control of the counting and chain of custody for secret vote counting are often the very same public officials caught in financial cheating. And should we really be surprised? Human nature is imperfect. The founders of this nation realized that, and precisely for that reason, envisioned a system based on distrust, not trust.

Bev Harris

(Bev Harris is author of "Black Box Voting", described as "the bible" of electronic voting by the Time magazine and a champion of voters' rights who has been called "the Erin Brockovich of Elections".)

The whole world, except we in India, is alive to the dangers of insider fraud in elections, mostly by insiders in the electronic voting machine industry. Jimmy Carter,

former president of the U.S. and James Baker III, former secretary of state, co-chairs of the Commission on Federal Election Reform, U.S. in their report titled, "Building Confidence in U.S. elections" said:

> "There is no need to trust the insiders in the election industry anymore than in other industries, such as gambling, where sophisticated insider fraud has occurred despite extraordinary measures to prevent it."

Role of Private Players

The Election Commission's guidelines make checking of EVMs mandatory before their use in elections. In its letter dated October 12, 2007, the Commission wrote to the chief electoral officers of states:

> "the Commission has decided that 'First Level Checking' of EVMs before elections shall be done by authorised engineers / technicians of BEL or ECIL as the case may be."

The letter further elaborates the reason for this decision saying, "In the past it has been noticed that malfunctioning of various switches comes to notice soon after the commencement of poll leading to the suspicion that possibly all switches have not been checked during pre poll check."

With this decision, the Election Commission of India had handed over to the manufacturers, the BEL and ECIL, two very crucial functions in the conduct of elections viz. manufacture of EVMs and their maintenance or checking.

BEL and ECIL, it is gathered, engage private players for first level checking and preparation of the EVMs who remain in the allotted districts to do trouble shooting during polling and counting stages. On an average, 10

such technicians are engaged per district. According to the grapevine, some of these private players engaged by the EVM manufacturers are close associates and relatives of political leaders.

Both the Election Commission and the EVM manufacturers have refused to divulge any information in this regard despite repeated requests. There are many questions that remain unanswered: who were the persons engaged for this activity; what procedure was adopted to appoint these "authorised" technicians and what were the terms of their engagement?

The Election Commission has given total functional autonomy to the EVM manufacturers and they are free to decide which group of technicians goes where. The Election Commission and the Chief Electoral Officers are merely given a list of technicians deputed to a district and the dates of their field visits.

Why has the Election Commission not considered it prudent to have checks and balances in election operations by engaging independent agencies (like the NIC for instance) for certification of EVMs rather than relying on the same PSUs manufacturing them?

The Election Commission exercises unlimited control over officials engaged in election duty; monitors their functioning very closely and punishes them for any deviations. That being the case, what had prompted the Commission to place boundless trust in the manufacturing PSUs over whom it has no direct administrative control, whatsoever?

I have raised many questions in this chapter that have serious implications for the security of the electronic voting machines and hence the integrity of election outcomes. Ignoring these would seriously imperil our democracy.

Voting machines must remain in a secure environment throughout their life, not just when the election process is underway. If the security is lax, at any stage in the life cycle of the voting machines, they can be hacked and kept ready for manipulation before next elections.

13

Weak Links in the Chain

If something can go wrong, it will.
Murphy's Law

It is not merely the vulnerabilities of the software and hardware of EVMs that are a matter of concern. There is a very long chain of custody of EVMs involved in the conduct of elections. And, there are so many weak links in the chain.

Lax Storage

The Commission's Handbook for Returning Officers (2009) says, "As a general policy, the Commission desires that all EVMs available within a district shall be stored at the district headquarters under the direct control of the District Election Officer or in a decentralized manner in different locations."

Officers under whose charge electronic voting machines are stored in districts are under the direct control of the respective state governments. Only during the period of elections, these officials are brought under the control of the Election Commission.

Security of voting machines throughout their life cycle is of paramount importance. "Voting machines must remain secure throughout their entire service lifetime", said Hovav Shacham, professor of computer science in the University of California, U.S whose team had demonstrated how hackers can steal ballots from electronic voting machines.

Thus, voting machines must remain in a secure environment throughout their life, not just when the election process is underway. If the security is lax, at any stage in the life cycle of the voting machines, they can be hacked and kept ready for manipulation before next elections.

The Election Commission's real concern for the security of voting machines begins only when the polling process begins. This is evident from the Commission's communication to the CEOs of states and Union territories dated 12th October, 2007. It reads:

> "The Observers deputed by the Election Commission on their arrival in the district shall inspect along with the District Election Officers (DEOs) and Returning Officers (ROs) the storage center for the EVMs in the district and randomly check the stock register with the stock stored."

Merely checking the stock registers does not offer any protection against detecting any tampering that may happen during their long period of storage between two elections in the storage centers. Further, as election Observers are appointed only a month before polls and they reach districts only weeks before polling, the security of the EVMs – often stored at many places within a district due to constraints of storage space – remains a matter of concern.

Electronic voting machines stored in a same district are commonly used in the same district for several elections. This means that if one is able to gain access

to the EVMs stored in a particular district and tamper with them at any time before the next elections, one would be in a position to alter the election outcomes in that district. This is a pretty scary prospect.

As the EVMs owned by the Election Commission of India are used only in assembly and Lok Sabha elections, ideally, they should remain under the direct control of the Election Commission at the national level and not in the districts and blocks with inadequate security arrangements.

Poor Randomization

The Election Commission says that it does not matter where EVMs are stored as allotment of EVMs is done through a process of randomization, which makes it impossible for anyone to know in advance where a particular EVM would be deployed. This, the Commission believes, acts as a deterrent against hacking as the hackers wouldn't know in advance where a manipulated EVM is likely to be used.

The process of randomization adopted by the Commission doesn't offer much protection. This is how it is done. Within a district, EVMs are first allotted randomly to different assembly constituencies and then to different polling stations within an assembly constituency.

What all this means is that any party or candidate wanting to manipulate EVMs would not be able to able to choose the target well in advance as the randomization process is completed only a few days before polling. This, however, assumes that parties/candidates would want to manipulate results only in select booths. If a political party can manipulate elections in its favor in the entire district, would not be tempted to do so?

Further, many Lok Sabha constituencies are as large as districts. In such cases, randomization of EVMs

within a district serves little purpose as every EVM in the district is likely to be used in the same parliamentary constituency.

Randomisation of EVMs at district level offers little protection. National level randomization would be better. However, even that cannot be a guarantee against manipulation of election results. The only way to prevent tampering of EVMs is by undertaking a software and hardware audit of all the EVMs before their use in the elections and allowing third party inspection and verification.

Inadequate Checking

As the EVMs are stored in districts for long periods and their use is rather infrequent, checking them before their use in every election becomes important to be sure that they have not been tampered with. In this regard, the following observation of the Technical Experts Committee of the Election Commission in its 2006 report is very significant:

> "...as a preventive measure, the Committee recommends that before every election, the manufacturers may be asked to check and ensure that all the units are functioning as designed. Incidentally, this method will be checked, by what is called the 'self test signature of Machine' and thereby the Manufacturers will be able to certify that the Machine is identical to what they have supplied and it has not been modified or replaced by any other."

The Election Commission has not implemented the recommendation of its own Expert Committee in this regard. Electronic voting machines are checked before every election following the guidelines issued by the election Commission. This is referred to as "First Level Checking" and involves checking of all the switches and buttons of the EVMs to ensure that they are working

properly. This also involves checking the functionality of the EVMs by polling 10 or more dummy votes. (Election Commission's letter to CEOs of states dated October 12, 2007)

The checking protocol suggested by the Election Commission does not include 'self test signature of Machine' recommended by the Expert Committee to establish that the machine is identical to what they (the manufacturers) have supplied and it had not been modified or replaced by any other. This would have been possible with the help of an "Authentication Unit," a project that was aborted by the Election Commission after the prototype was developed, tested and readied for use. Details of this have been discussed in chapter 2. This is a glaring security lapse. Repeated questions have failed to elicit any response in this regard.

The "first level checking" protocol prescribed by the Election Commission is a mechanical check and offers no protection against either software manipulation or replacement of hardware. Ironically, even these basic checks are not carried out properly on EVMs. Why else would hundreds of EVMs fail to perform properly in elections? I have cited several such cases in chapter 4.

Deficient Training

A presiding officer, who is typically a Gazetted Officer or at least a supervisor level government official, is usually in charge of a polling station. A team of usually three polling personnel assist him in manning a polling station on the day of polling. They are expected to set up the EVM in the polling station by connecting ballot and control units, operate the EVM and attend to all its problems in addition to their regular duties.

Election Commission prescribes the following guideline in respect of training of polling staff in the use of voting machines:

> "It is essential that thorough and intensive training is imparted to the election machinery in the use and operation of voting machines...You should hold polling rehearsals as often as possible where the use and operation of the voting machines should be explained and practically demonstrated. You should see that every Presiding Officer... attends at least two or three such rehearsals and is given an opportunity to have "hands-on" training on the machine. (Item 6.1 on page 12 of the Handbook of Returning Officers)

The Election Commission's above guidelines on training of polling personnel are vague. Presiding officers attending these training programmes say that the training is more of a formality and not a serious affair. There is no standardized content or structure for the training. The technical manpower available for training presiding officers on the operation of the voting machines is inadequate.

As a result of poor training, polling officials face a lot of problems in handling voting machines at the time of polling. Presiding officers are given classroom training in large batches in conference halls and get no practical training at all.

"We are given a briefing about the functions and operation of the voting machines in large groups and told to read detailed notes given in the presiding officers' diary. Each group of 10 persons is given one voting machine to practice on our own on the voting machine. Then, we are asked to sign in a register that we have understood everything. On paper, you cannot find fault with the training process but in reality, it is woefully inadequate" says Vinay Kumar, a teacher who worked as a presiding officer in the recent Jharkhand assembly elections.

P. K. Gaikwad, who worked as a presiding officer in the recent Maharastra polls says, "The entire training

lasts for a period of three hours. A group of five to ten officials are given one machine and told to practice on it. The hands-on-training on the machines is not at all adequate." He adds, "Every presiding officer must be given a separate voting machine and asked to practice and demonstrate machine operation under the supervision of experienced trainers."

The Election Commission is aware of the pitfalls of training but conveniently shifts the blame onto the officials. The Commission says:

> *"It has further come to the notice of the Commission that some of the Presiding Officers / Sector Magistrates do not take EVM training seriously with the result that they fail to operate the machine at the time of poll." (Election Commission's letter to CEO's dated 21st January, 2009)*

Ineptness of Officials

It is not just lowly presiding officers, but even senior officials at the level of Returning Officers exhibit ineptness in handling voting machines. The Election Commission acknowledges that the polling officials face problems in operating voting machines due to problems in the preparation of voting machines at the Returning Officer's level.

> *"During previous elections, it has come to the notice of the Commission that there were some difficulties in the operation of the electronic voting machines at a few polling stations due to the fact that they were not prepared correctly as per the operational manual at the time of initial preparation at the Returning officer's level." (Election Commission's letter to CEO's dated 21st January, 2009)*

The above observations of the Election Commission point to a glaring admission that government functionaries involved in the poll duty-even at the level of Returning Officers–face difficulties or exhibit

ineptness in the preparation of voting machines many years after the voting machines have been introduced.

Wrong "preparation" of voting machines can have disastrous consequences and lead to votes of one candidate getting recorded in favour of another.

In constituencies where the number of contesting candidates exceeds sixteen, more than one ballot unit is connected or linked to each control unit. The ballot units have a 'side switch' which has to be set properly. The second ballot unit, i.e., the ballot unit in which the slide switch is set at position 2, is linked with the first ballot unit in which the slide switch is set at position 1 and so on.

While setting these switches on the ballot units, if the 'side switch' is set in the wrong position at the time of preparation of voting machines, the votes of one candidate will get delivered to another in the same position on the wrongly linked ballot unit.

The Commission's letter of 21st January, 2009 acknowledges such incidents are not uncommon. The letter said,"While in some (voting machines) 'side switch' on the balloting unit was found to be in wrong position, in others, certain other preparatory defects were noticed."

Another problem of improper inter-linking relates to a mix up of control units in case of simultaneous assembly and Lok Sabha elections. If the ballot unit(s) meant for assembly election are linked with the control unit of Lok Sabha and vice versa, the consequences would be disastrous. For instance, the votes of first candidate on the ballot paper for assembly election will get delivered to the first candidate in the Lok Sabha election and likewise.

Non-Conduct of Mock Poll

According to the guidelines of the Election Commission, a mock poll is to be carried out on every

EVM before the commencement of the actual poll in the presence of the polling agents of candidates. The election petition filed by the Congress candidate in Orissa had alleged, "The mock poll was not carried out at the polling stations before the commencement of the actual polling." Similar complaints were reported from several places across the country.

A letter issued by the Election Commission dated 22nd April, 2009 – on the day of second phase of polling for 2009 general elections – suggesting that a mock poll need to be conducted only when a control unit is replaced caught my attention. The Commission's letter reproduced below said, "Mock poll is not required to be conducted when only Ballot Unit is replaced, as Ballot Unit has no polled memory data." Significantly, this was the day when Orissa went to polls.

ELECTION COMMISSION OF INDIA

Nirvachan Sadan, Ashoka Road, New Delhi-110001

No.51/8/7/2009-EMS Dated: 22nd April, 2009

To
The Chief Electoral Officers of
All States and Union Territories.

Reference: Commission's letter No.51/8/7/ 2009-EMS, dated 8th April, 2009.

Subject: Clarification on conduct of mock poll in case of replacement of EVM.

Sir,

I am directed to refer to the Commission's letter No.576/3/2009/SDR, dated 5th January, 2009 on the subject cited and to clarify that mock poll should be conducted only when the Control Unit is replaced. Mock poll is not required to be conducted when only Ballot Unit is replaced, as Ballot Unit has no polled memory data.

Yours faithfully,
(K.N.Bhar)
Under Secretary

I am curious as to what made the Commission to issue such a letter. In chapter 11, I have described how easy it is to manipulate ballot units by tampering with the Programmable Logic Devices (PLDs). Given this serious vulnerability of the ballot units, it is important that every ballot unit is checked before its use in elections.

Not testing ballot units after their replacement through a mock poll is a security hazard and it is not clear what prompted the Commission to issue such a directive.

Tallying of Votes by Poll Officials

Our enquiries from across the country have revealed that polling officials suspend polling for sometime saying the EVM had developed some complication and resume polling after some time, raising suspicion among the voters that they may be manipulating the results. As the presiding officers have little knowledge about the EVMs and know only how to operate them, it is unlikely that they are repairing the EVMs when they suspend the polling operation. What are they doing then?

It is possible that they may be tallying the manual count of votes as recorded in the register and an electronic count that becomes known by pressing the "Total" button on the control unit. This they are required to report every two hours on the polling day total number of votes polled. Here are the instructions in this regard from the Handbook of Presiding officers:

What do the presiding officers do if there is a discrepancy between the manual count from the register and the electronic count from the control unit? Some presiding officers may cast some votes on their own to match the number in both counts! Is that the reason why the polling officials stop polling in between? May be, yes.

Tallying of number of votes polled periodically

4.1 At any time, if the total number of votes polled up to that time has to be ascertained, the 'Total' button on the control unit should be pressed. The display panel on the control unit will then show the total number of votes polled by that time. This should be periodically done and tallied with the number of electors allowed to vote up to that time as reflected in the register of voters.

4.2 In any event, you must ascertain and tally the number of votes polled during every two hours interval and record the number of votes polled in the relevant columns in the Presiding Officer's diary.

Discrepancies in Votes Polled & Counted

After the close of poll, the voting machine and all election papers are sealed. Polling agents of candidates present at the polling station are also allowed to affix their seals on the voting machine and the election papers. The following are the ECI instructions in this regard.

CHAPTER XXXI
SEALING OF THE VOTING MACHINE AFTER CLOSE OF POLL

1.3 Each carrying case should then be sealed at both ends by passing a thread through the two holes provided for the purpose on both sides of the carrying case and putting thread seal with an address tag showing the particulars of the election, the polling station and the unit contained therein and carrying the Presiding Officer's dated signatures & seal on it.

1.4 The particulars on the address tag on the control unit and ballot unit shall be the same as mentioned in para 2(1) of chapter III. The contesting candidates or their polling agents, who are present at the polling station and desirous of putting their seals on the address tag, should also be allowed to do so. (Handbook for Presiding officers)

Many polling agents have told us that this practice serves no purpose as the polling agents are not present at the counting centres. Counting agents of a candidate are not in a position to personally verify the signatures of their polling agents. As a result, any malpractices like replacement or tampering of control units after polling would go uncontested by the candidates. The hurried manner in which the electronic counting is taken up without verifying the authenticity of the control units is a matter of great concern.

Counting Day Manipulations

> "Everybody watches polling closely and nobody watches counting," says Bev Harris, author of Black Box Voting in the context of U.S. elections.

In my assessment, what Bev Harris says is equally true of Indian elections as well, particularly after the introduction of EVMs. Our Election Commission takes three months to conduct parliamentary elections but wants counting to be over in just three hours! Why this great hurry? Fast reporting of results ought not be a priority at the altar of accuracy and integrity of elections.

In the rush to declare results and the winners, several serious lapses go unnoticed in the counting process. Field reports suggest that there are several polling stations across the country where there are discrepancies between the number of votes polled (as stated in Form 17 C given to polling agents after the polls close) and the number of votes counted in the EVM on the counting day.

This is strange as the votes polled cannot disappear in thin air and votes not polled cannot find their way into the EVM when the control units are kept securely in the strong rooms. But these have happened and in several instances. I have referred to several such

instances in chapter 4, including a Times of India report on Maharashtra assembly elections in which the number of votes counted exceeded the votes cast!

This is indeed a serious issue and establishes that the EVMs may have been manipulated after the polls have closed. Is that possible when the EVMs are stored in strong rooms under security? That is a question that the election officials and the Election Commission must answer. Such questions remain unanswered as once the counting is over and the winners and losers are declared. If the Indian EVMs are fail safe and fool proof, as the Election Commission believes, why would such discrepancies occur? Why has the Election Commission not conducted an enquiry into such cases to identify and fix the problem?

Non Issuance of Form 17 C

The election rules stipulate that presiding officers must hand over signed copies of Form 17 C to the polling agents of all the contesting candidates. But in many polling stations across the country (specifically in states like Orissa), it is alleged that Form 17 C was not even issued to the polling agents. This was cited prominently by the Congress leaders in their election petition in the Orissa High Court*.

Political Parties Need to be Alert

Even a decade after their extensive use in elections, political parties have not understood how to protect their interests in the EVM regime. Due to their lack of knowledge and blind faith in the fairness of the election administration, candidates and parties tend to neglect many critical activities involving EVMs.

The person who is usually made in charge of dealing with the EVM related matters is certainly not the most capable person with a proper capacity to understand

** See Annexure 7*

things. These tasks are assigned to persons who are generally considered not good for anything else. With such a casual approach, the monitoring of EVMs becomes a casualty.

Parties and candidates need to be alert in several aspects. Election Commission guidelines allow candidates or their representatives to be present and monitor several activities like randomization of EVMs, preparation of EVMs, checking of EVM serial numbers before their use at the polling station, mock poll, issuance of Form 17 C, sealing of control units after polls, security of strong rooms etc.

By not taking these activities seriously and blindly relying on the fairness of the district officials, candidates would be taking a huge risk of potential insider fraud. Although these activities alone may not offer total protection against insider fraud, not taking these activities seriously would increase the risk of manipulation.

In polling stations, when a mock poll is carried out by presiding officers, polling agents are not always present. If the polling agents are not properly trained to monitor this activity, there is scope for the presiding officers to indulge in malpractices. The polling agents, even when they are present, are too scared to raise any objections against presiding officers as they do not want to 'antagonise' them for fear of retaliation.

***

Even if a political party is alert, there are many ways in which EVMs can be hacked.

14

Hacking EVMs, Hijacking the Mandate

The Indian EVMs can be hacked both before and after elections to alter election results. In this chapter, I have referred to different ways of manipulating Indian EVMs; before and after elections. There may be many more ways to do it. Hacking, after all, is a creative activity and there are no bounds to creativity. Indian EVMs have left so many holes in their security that any creative hacker would love to exploit their vulnerabilities.

Possibilities Before Elections

Before elections, a hacker can attack the voting system in two ways; one by tampering the original source code fused onto the microchips in the control unit or by attacking the ballot unit.

For tampering the original source code, the hacker will have to either gain access to the original source code used in the EVMs or decode it through reverse engineering process. Alterantively, he may write his own

code to make the EVM function. Through any of these methods, the hacker would be able to gain control of the EVM and can do whatever he wants with it.

Even more easier would be to hack the ballot unit. Ballot units have Programmable Logic Devices (PLD) which contain keyboard logic. When the keys on the ballot unit are pressed to choose a candidate at the time of polling, the logic sends key codes to the microchip inside the control unit which in turn redundantly writes it into two EEPROMs present in the control unit. EEPROMS are the chips where the voting data is stored.

A hacker with even basic skills can easily read the logic in the PLD chips by using a simple logic analyzer and can change the logic. The manipulation possibilities are endless. One way to manipulate logic is to say that every n^{th} vote should get delivered to a particular key or candidate.

This data manipulation logic can be coded such that it gets activated only after a certain number, say 100 votes are polled. As only a few votes are polled in mock polls to check the functionality of the EVM, such tampering would go completely unnoticed. Moreover, ballot units are not even examined after polling and everybody feels that it is only the control unit that needs to be secured.

Large scale problems with regard to the functioning of the ballot units in many places (specifically in states like Tamil Nadu) prima facie appear to be a case of tampering of the ballot units on a large scale. As the tampering was not done perfectly, the ballot units misbehaved at many places. If an audit of all the misbehaving ballot units is ordered, the truth will perhaps be known. The Election Commission must undertake such an audit to restore the confidence of political parties and public in a voting system about which many concerns exist.

After Elections

If a hacker has not manipulated EVMs before polls, there are two post poll hacking options available.

First, this can be done by directly attacking the storage devices called EEPROMs in the control unit. This is where the voting data is stored. They are completely unsecured and the data inside EEPROMs can be manipulated from an external source with ease completely bypassing the embedded program in the microcontrollers. It is very easy to read (data from) the EEPROMs and manipulate them. As these are commonly used storage devices, information on them is publicly available on the worldwide web.

The second and the most dangerous way to manipulate Indian EVMs was revealed to me by Dr. Alex Halderman, professor of computer science at the University of Michigan, who would be present at the launch of this book in New Delhi. Says he, "Hacking Indian EVMs is easy. They can be hacked by just inserting a simple 8 pin chip behind the display section of the control unit, which would go unnoticed. When the results button is pressed on the counting day and the results begin to flash on the display screen of the control unit, the Trojan in the inserted chip may get activated."

As soon as the total number of votes polled in the EVM is displayed by the machine in the display screen, the Trojan would instantly manipulate the votes of all other candidates and display the manipulated counts. How you want to manipulate the results is your choice. The Trojan would do whatever you want with it.

The Trojan can be programmed such that it gets activated only when the total number of votes exceeds a specific number, say 100. This would ensure that the presence of such a Trojan does not get highlighted during mock polls.

"Indian EVMs can be hacked by introducing Trojan in display unit"

Dr. Alex Halderman is Computer Science Professor at the University of Michigan. He is a noted expert of Electronic Voting Security who demonstrated first voting machine virus, lead team of Scientists from Princeton and Berkeley for "Top to Bottom" review of California EVMs.

With so many vulnerabilities, Indian EVMs can be a hacker's delight. An expert with the knowledge of the Indian EVMs quips, *"Indian EVMs are like the Iraq strongman Saddam Hussein hiding and getting caught in a bunker."*

EVMs are Sitting Ducks

This list of vulnerabilities of ECI-EVMs is based on inputs from knowledgeable people in the industry who are aware of the myriad vulnerabilities of Indian EVMs. The list may not be exhaustive.*

1. "Generic" microchips which contain the 'secret' software can be replaced with tampered chips to manipulate the functioning of the EVMs.
2. The mother board (or card) of the control unit of the EVM are snap-fit and can be removed at a click and replaced with new cards having tampered chips.
3. The entire EVM can be replaced with a fake one having a malicious program. This can happen either before or after polls.
4. There are 2 EEPROMs inside each Control Unit in which the voting data is stored. The voting data can be manipulated from an external source with ease bypassing the "secure" microchip.

5. EVMs can be hacked by changing the keyboard logic contained in the Programmable Logic Devices (PLD) inside the ballot units to manipulate their functioning.
6. A jumper inserted at the ballot unit end in the cable that connects to the control unit can divert all votes in favour of a particular key or candidate in whose behest the election is to be fixed.
7. EVMs can be hacked by inserting a chip with Trojan inside the display section of the Control unit. Bypassing completely all inbuilt securities, this chip would manipulate the results and give out "fixed" results on the EVM screen.
8. If the microcontrollers in the EVMs are embedded with a Bluetooth device or a micro-transmitter, it is possible to manipulate the EVM through remote devices. This would be possible only with collusion of insiders.

** Not all these vulnerabilities are present in every EVM as there are variations between different makes and models.*

Voting machines at elections: Notwithstanding anything contained in this Act or the rules made there under, the giving and recording of votes by voting machines in such manner as may be prescribed, may be adopted in such constituency or constituencies as the Election Commission may, having regard to the circumstances of each case, specify. (Section 61A, The Representation of the People Act, 1951)

15

Are Indian EVMs Constitutional?

Use of electronic voting machines in elections was declared "illegal" by the Supreme Court of India in 1984. Surprised! Read on.

Electronic voting machines were first introduced in the country in 1982 in assembly elections on a limited basis. One such constituency where they were used was the Parur Assembly constituency in the state of Kerala. In 50 of the 84 polling stations, electronic voting machines were used. The defeated candidate A.C. Jose who polled 30,327 votes and lost the election to Sivan Pillai by a small margin of 123 votes appealed in the Supreme Court alleging that the use of electronic voting machines in elections was illegal and prayed that the election be set aside. (A.C. Jose vs. Sivan Pillai – 1984 (2) SCC 656.)

Supreme Court held EVMs Illegal

On March 5, 1984, in the A.C. Jose vs. Sivan Pillai-1984(2) case, the Supreme Court of India had ruled that

the use of EVMs was illegal and that the Election Commission had no power to use electronic voting machines as the Representation of People Act (RPA), 1951 and Conduct of Election Rules, 1961 only provided for use of ballot papers and ballot boxes in elections.

Thus, the Election Commission's initial attempts in 'imposing' electronic voting machines on the country without relevant provisions in the statute met with a scathing indictment by the highest court of the country. Justice Murtaza Fazl observed:

> "If we were to accept the contention of the respondents (Election Commission), it would convert the Commission into an absolute despot in the field of election.... If the Commission is armed with such unlimited and arbitrary powers....bring about a constitutional crisis, setting at naught the integrity and independence of the electoral process, so important and indispensable to the democratic system." (AIR 1984, SC 921, Para 21)

In 1989, the Representation of People (RP) Act, 1951 was amended by Parliament incorporating Section 61A which allowed use of electronic voting machines. With this change of statute, the Election Commission re-introduced EVMs in Indian elections. But, the question arises: did the amendment empower the Election Commission to introduce them on a nationwide scale as it did in 2004 and 2009.

2004 & 2009 Lok Sabha polls Illegal?

The amendment made to the RP Act in the form of 61A in 1989 allowed use of EVMs selectively and did not envisage blanket use of EVMs on a universal basis.

The amendment to the act states that voting machines "may be adopted in such constituency or constituencies as the Election Commission may, having regard to the circumstances of each case, specify."

The amendment reads as follows:

> "61A. Voting machines at elections: Notwithstanding anything contained in this Act or the rules made there under, the giving and recording of votes by voting machines in such manner as may be prescribed, may be adopted in such constituency or constituencies as the Election Commission may, having regard to the circumstances of each case, specify". (The Representation of the People Act, 1951)

Further Explanation provided Section under 61 A in the RP Act reads as follows:

> Explanation.-For the purpose of this section, "voting machine" means any machine or apparatus whether operated electronically or otherwise used for giving or recording of votes and any reference to a ballot box or ballot paper in this Act or the rules made thereunder shall, save as otherwise provided, be construed as including a reference to such voting machine wherever such voting machine is used at any election.

The explanation makes it further clear that the amendment made in the RP Act envisaged that both the voting systems – ballot papers and voting machines – would continue to co-exist and that voting machines will be used with regard to the circumstances of each case. A similar system works in some countries in Europe (for instance in France) where electronic voting machines are used in a limited manner in select constituencies. Similarly, Indian law makers visualized use of EVMs only in select constituencies or on a limited basis.

It was not in the powers of the Election Commission to conduct nationwide elections through electronic voting machines violating this provision under the R.P.

Act. This becomes clear from the Supreme Court's ruling in the A.C. Jose vs. Sivan Pillai case, 1984. In its judgment, the Court stipulated the limitation to the powers of the Election Commission under the constitution. It said:

Supreme Court's Observations on the Powers of the Elecion Commission

"To sum up, therefore, the legal and constitutional position is as follows:

(a) When there is no parliamentary legislation or rule made under the said legislation, the Commission is free to pass any orders in respect of the conduct of elections,

(b) Where there is Act and express Rules made thereunder, it is not open to the Commission to override the Act or the Rules and pass orders in direct disobedience to the mandate contained in the Acts and Rules.

(c) Where the Acts and Rules are silent, the Commission has no doubt plenary powers under Article 324 to give any direction in respect of the conduct of elections and

(d) Where a particular direction by the Commission is submitted to the government for approval, as required by the Rules, it is not open to the Commission to go ahead with implementation of it at its own sweet will even if the approval of the government is not given."

Clearly overriding the provisions under the R.P Act and deviating from the stated legal and constitutional position enunciated by the Supreme Court of India, as above, the Election Commission had conducted 2004 and 2009 parliamentary elections using EVMs in all constituencies of the country.

Election Commission officials claimed in discussions that all political parties agreed to the use of EVMs throughout the country in the All Party Meeting held

on February 3, 2009 before the April-May, 2009 general elections. This, the Election Commission believes has granted them the legal sanction to use EVMs all over the country. *This reasoning is unacceptable. When have all party meetings acquired legislative powers?* Where is the need for any legislation if the Election Commission and political parties can mutually agree on electoral laws and reforms in All Party Meetings?

The Election Commission seems to be in violation of legal provisions once again, as earlier in 1982. The Supreme Court then held that the election to the Parur Assembly constituency in Kerala was illegal and set aside the election on the grounds that that it was conducted violating the provisions of the R.P. Act.

For a similar violation and using EVMs on a national scale, shouldn't the parliamentary elections of 2004 and 2009 be also held illegal? Judge it for yourself.

Constitutional Issues

Besides the technical and legal considerations, there are larger constitutional issues involved in the use of electronic voting machines in elections. They may be held unconstitutional because they – EVMs store voting data only on electronic memory devices – infringe the fundamental rights of the voters. Here go the arguments.

True, the right to vote is a legal right, given under the Representation of People Act and it is not a fundamental right. But how that vote should be exercised by a voter is his/ her individual expression and that is covered by Article 19 (1) (a) of the Constitution, which guarantees fundamental rights to the citizens of the country. It is this fundamental right, the human right of a voter which is required to be preserved & expanded, if we want to make democracy vibrant and live.

Relevant in this regard is the 2002 judgment of the Supreme Court of India in the case pertaining to

disclosure of assets and the criminal background of candidates. The Supreme Court emphasized that the voter has the right to know the antecedents of the candidates before making his choice so that the choice is not mechanical but an informed choice. The Supreme Court reasoned:

> "**Under our Constitution, Article 19(1) (a) provides for freedom of speech and expression. Voter's speech or expression in case of election would include casting of votes**, that is to say, voter speaks out or expresses by casting vote. For this purpose, information about the candidate to be selected is a must. Voter's right to know antecedents including criminal past of his candidate contesting election for MP or MLA is much more fundamental and basic for survival of democracy."

Legal experts say that the emphasis should be on making this right absolutely free and transparent from all hurdles created by law and procedure. "A voter has the right to know that his vote which he exercised as a part of freedom of expression to sub-serve the democracy has really gone in favour of the candidate whom he/ she has chosen. This right which is fundamental in nature and not merely a legal right is completely absent in the electronic voting system," says Sanjay Parikh, Senior Lawyer, Supreme Court.

In the traditional paper ballot system, that fundamental right was preserved because a voter knew exactly how his/ her vote was recorded and counted. Seen in this light, the use of EVMs in Indian elections is liable to be held unconstitutional. There is a clear international precedent for this in the decision of the Federal Constitutional Court of Germany in March 2009.*

** See Annexure 2*

Legal Challenges in India

A question is bound to arise in your mind. If this is indeed so, why have the Indian courts not ruled on this matter yet?

Though a number of public interest litigations and election petitions have been filed in the Supreme Court of India and several High Courts, the focus of these litigations has largely been on the vulnerability and tamperability of electronic voting machines and less so on the larger constitutional issues concerning fundamental rights of voters. As most of the questions raised were of technical nature, the Courts have routinely referred the matter to the Election Commission to hear the "complaints".

If a proper legal challenge is mounted questioning the constitutionality of the electronic voting machines, I am confident that the Indian Courts will examine the constitutionality or otherwise of electronic voting in Indian elections. Such challenges are already in the offing.

"German Judgment Applies to India"

By Paul Lehto*

The principles discussed in the German Court ruling do apply to all countries, because essentially all countries are formally and legally committed (even if not in fact acting this way) as republics or democracies. Under the Universal Declaration of Human Rights, not to mention countless national documents and rights (whether written or not) around the world, the only legitimate source of (governmental) power is the people's mandate. As the ultimate source of all legitimate power, when the people transfer that power in elections, they are acting in a very powerful and

special way: as co-sovereigns selecting their public servants.

Here is only one principle from which ALL else flows: We the People are sovereign. Or "in charge" or "the boss" or "the ultimate power" or whatever you want to call it.

From this one single principle of power from the people – the denial of which exposes the denier as undemocratic – everything else follows and rolls downhill so to speak.

This principle is really not contestable when you consider what BETTER claim could any subset of people have to rule over us? Anyone claiming such power is an aristocrat or oligarch at the very least, quite possibly wants dictatorship.

If we are sovereign, then we must be able to control our own elections. If that's rendered impossible or difficult, then our sovereignty is implicitly denied.

The German opinion is a reflection of this kind of thinking, as it notes that there is no substitute for public transparency of all essential features.

I'm sure the Indian court, if presented with the above considerations, would agree that the people are in a uniquely powerful position in elections, leading to very unique dynamics in voting whereby any non-transparency is a direct denial of people's rights and thus a denial of democracy.

(Paul Lehto is a noted Attorney and election reform advocate. He is a former governor of the Washington State Bar Association, USA)*

16

Restore Transparency and Verifiability

It's not voting that's democracy, it's the counting.
Tom Stoppard

The earlier chapters of this book have documented the numerous vulnerabilities of the electronic voting machines (EVMs) used in our elections and instances of their large-scale failures during polling.

The Election Commission of India has been largely dismissive of the serious misgivings among political parties, candidates and citizens' groups about electronic voting. Elections are all about trust. If the losers and their supporters do not trust the election results and is there is no "physical evidence" or basis to show that their fears are unfounded, the legitimacy of election results would remain perpetually under a cloud.

Rationale of the German Judgment

This was the rationale behind the landmark judgment of the Federal Constitutional Court of

Germany in March, 2009 which held the use of electronic voting machines in Germany unconstitutional.

It based itself mainly on 'the principle of the public nature of elections' in a democracy - that all essential steps of an election are subject to the possibility of public scrutiny. It is not sufficient to say that the voting data is stored in the voting machine and an electronic display or printout is possible, and that election officials are carrying out necessary tests and vouching for the security and technical integrity of electronic voting machines.

The process should be transparent in a manner that the general public can be satisfied that their vote is correctly recorded, and the standard the Court set for this purpose was that there should be a provision whereby 'the votes are recorded in another way besides electronic storage' and there is 'retraceability' of the election result independently of the electronic count.

In other words, the Court ruled that EVMs are unconstitutional so long as there was no provision for an additional verifiable physical record of every vote cast.

It should be evident that the principles enunciated by the German Court are universal ones applicable to all democracies. The common man is often confused and intimidated by the beeps and flashing lights of technology, and has no means of knowing what goes on inside the 'black box' voting machine. While this would be true anywhere, such a consideration should have even greater force in India where a large section of the electorate is illiterate and disadvantaged.

Essential Elements for Credible Elections

On the basis of experience with voting machines around the world, three essential elements have come to the fore as universally important for a voting system

to be considered credible. They are:

Transparency: Voters should be able to 'observe' the voting and counting process without any specialized knowledge, feel confident that their vote has been correctly recorded and would be fairly counted, and that any occurrence or attempt to commit electoral fraud would be easily detected by general public.

Verifiability: Voters should be in a position to verify in case of a recount, through a proper examination of the physical record of ballots, whether the declared result was the same as the actual vote.

Accountability: If anything with the election process goes wrong, the voting system should be such that it can be detected instantly, responsibility can be fixed clearly, and remedial steps can be initiated immediately.

When all the above three elements are guaranteed, the voter finds the system trustworthy and is in a position to confidently exercise his "sovereign" power to elect his representatives and place in power a government of his choice.

In the traditional system of paper ballots, all these essential requirements were met adequately. However, the present electronic voting system in India does not meet any of these three elements.

In the present EVMs, voters have no way of knowing if their vote is recorded or counted properly. In case of any doubt, neither voters nor candidates can seek a genuine recount as no physical record of votes is generated and all voting data is stored only on electronic memory devices, which voters and candidates cannot be sure have recorded their votes correctly. And, if something goes wrong with the recording or counting of an election, there is no means of detecting it or proving it. And of course fixing responsibility is out of the question and no one can be held accountable in this non-transparent, unverifiable system.

Ironically, the electronic voting machines have rendered voters totally powerless and made the officials and agencies involved in the conduct of elections supremely powerful. What would you call it but a travesty of democracy where the people supposedly enjoy "sovereign" power to elect their public representatives?

The present system of non-transparent, secretive, elitist and "faith based" electronic voting must make way for a more open, transparent system of voting to make Indian elections credible.

What should we do? What alternatives do we have?

Paper Ballots are the Gold Standard

Today, use of paper ballots and hand counting of votes – which is what India followed for decades before the advent of electronic voting machines – is considered to be the gold standard all around the world. Most countries in the developed world, which have experimented with electronic voting for a while, have gone back to paper ballots owing to its superiority in ensuring free and fair elections.

A study in France where electronic voting systems are used in a limited way, a comparative study had shown that the electronic voting systems are prone to a much greater degree of error than paper ballots.

Quelle Surprise! E-Voting Fails in France Too!

A study conducted in France had shown that polling locations which use electronic voting machines exhibited a higher number of discrepancies than those using conventional paper ballots.

The study was conducted at over 21,000 polling stations by comparing electoral registers, which voters sign after voting, with the total vote counts from machines and paper ballots in several

elections. Discrepancies were found at almost 30 percent of polling stations that use electronic machines and only at about 5 percent of those using paper ballots.

The findings of the French study are hardly surprising to those of us who haven't been ignoring the exact same problems for years here in the U.S. The difference, of course, will likely come in the way that France – like other European countries, and decidedly unlike the U.S.– responds to the findings...

http://www.bradblog.com/?p=6169

VVPAT System

The next best thing to the paper ballot system is introduction of what is referred to as "Voter Verified Paper Audit Trail (VVPAT)" along with the use of electronic voting machines.

VVPAT refers to a system where by the voting machines produce a paper record (a print out) of every single vote cast by the voters on the voting machines. After casting the vote on the EVM, the voter will examine the physical print out for its accuracy and if satisfied that there is no discrepancy, deposit the vote in a ballot box. This would ensure that even if the machine is manipulated, you have the paper record to establish the election fraud. At present, whatever voting data the electronic voting machine contains-whether original voting data or manipulated-becomes the official record.

In the United States, 32 of the 50 states have passed legislations mandating verifiable paper record for all votes cast. Another six states are following this requirement even without a formal legislation. That means use of electronic voting machines is possible in these states in the U.S. only if they can generate a paper record. There is a federal legislation pending in the U.S. Congress that seeks to mandate the paper

record of every vote in the U.S federal elections.

India also needs a similar legislation like what most states have in the United States that makes physical record of every vote cast mandatory. There is no reason why it would not work in India.

There is a writ petition filed in the Delhi High Court by Dr. Subramanian Swamy, former law minister seeking direction to the Election Commission to introduce the VVPAT system in the electronic voting machines. The developments in the case will be keenly watched even as the Election Commission is resisting attempts to introduce transparency in the voting process.

The introduction of VVPAT regime should be accompanied by of the following minimal additional safeguards in the present electronic voting machines to prevent both external hacking and internal fraud. They are:

- Both hardware and software used in the EVMs should be in public domain
- An "Authentication Unit" must be developed and available to all concerned for testing the authenticity of the EVM software and hardware before their use in elections
- EVMs should remain only in the custody of the Election Commission and should be available for third party inspections
- Randomisation of EVMs should be done at the national level

Implementation of VVPAT would mean additional costs but it would ensure that our voting system with EVMs conforms to the three universal principles of transparency, verifiability and accountability. Thus, it would remove the 'trust deficit' in the system, allow the voters to exercise their 'sovereign' power confidently, guarantee candidates' recourse to a fair recount, and thus strengthen our democracy.

What if there is a mismatch between "electronic" and physical counts? There should not be any such deviation in the first place as every single electronic vote is printed out, verified and authenticated by voters. However, if a discrepancy is found, it establishes manipulation of the electronic vote and the physical record should prevail as it is more reliable and verifiable.

"Paper Trail to Prevail in Recount"

According to the decision of the German Federal Constitutional Court the voter needs to have the possibility to control the correctness of all votes, including both his own and every other voter's votes. Although paper trail systems might be acceptable in general, this does not mean that the electronic vote is the relevant one (in the event of diverging outcomes): If interested citizens demand a recount, the physical prints are the definitive ones in the case of a deviation from the electronic counting.

Till Jaeger

(Till Jaeger is the Attorney who argued the landmark case before the Federal Constitutional Court of Germany that resulted in banning of EVMs in German elections.)

Need for Public Debate

A healthy public debate and an active role played by several institutions--the judiciary, media, legislature and civil society-helped countries like Germany, Holland and Ireland in reforming their voting systems. They all have rejected stand-alone EVMs in favour of the traditional paper ballot system. Most states in the United States of America have ensured that wherever EVMs are used they are backed up by a paper trail and other safeguards to ensure the sanctity of electoral democracy.

India is vibrant democracy with an independent judiciary, a free and fearless press, and a clamorous civil society that is quick to rise in favour of any public cause. If this important issue of EVMs and election reform has not found salience so far, it is largely because of the mystique around techlnology in the popular mind, and the Election Commission's resoluteness in keeping all relevant information out of the public domain.

However, there is reason to think that this is changing. Political parties and citizens' groups are coming together to take up the iissue in a concerted manner and there are some serious challenges before the courts. It is to be hoped that the Election Commission of India would also change its approach and decide to become a part of the solution rather than ignoring the problem.

Annexure 1

Resolution on Electronic Voting

We are in favor of the use of technology to solve difficult problems, but we know that technology must be used appropriately, with due attention to associated risks. For those who need to upgrade, there are safe, cost-effective alternatives available right now, and the potential for vastly better ones in the future. For these reasons, we endorse the following resolution:

"Computerized voting equipment is inherently subject to programming error, equipment malfunction, and malicious tampering. It is therefore crucial that voting equipment provide a voter-verifiable audit trail, by which we mean a permanent record of each vote that can be checked for accuracy by the voter before the vote is submitted, and is difficult or impossible to alter after it has been checked. Many of the electronic voting machines being purchased do not satisfy this requirement. Voting machines should not be purchased or used unless they provide a voter-verifiable audit trail; when such machines are already in use, they should be replaced or modified to provide a voter-verifiable audit trail. Providing a voter-verifiable audit trail should be one of the essential requirements for certification of new voting systems."

We elaborate below.

In response to the need to upgrade outdated election systems, many states and communities are considering acquiring "Direct Recording Electronic" (DRE) voting machines (such as "touch-screen voting machines" mentioned frequently in the press). Some have already acquired them. Unfortunately, there is insufficient awareness that these machines pose an unacceptable risk that errors or deliberate

election-rigging will go undetected, since they do not provide a way for the voters to verify independently that the machine correctly records and counts the votes they have cast. Moreover, if problems are detected after an election, there is no way to determine the correct outcome of the election short of a revote. Deployment of *new voting machines that do not provide a voter-verifiable audit trail should be halted, and existing machines should be replaced or modified to produce ballots that can be checked independently by the voter before being submitted, and cannot be altered after submission. These ballots would count as the actual votes, taking precedence over any electronic counts.*

Election integrity cannot be assured without openness and transparency. But an election without voter-verifiable ballots cannot be open and transparent: The voter cannot know that the vote eventually reported is the same as the vote cast, nor can candidates or others gain confidence in the accuracy of the election by observing the voting and vote counting processes.

All computer systems are subject to subtle errors. Moreover, computer systems can be deliberately corrupted at any stage of their design, manufacture, and use. The methods used to do this can be extremely difficult to foresee and detect. Current standards and procedures for certifying electronic election equipment do not require unambiguously that equipment provide a *voter-verifiable audit trail. Without a voter-verifiable audit trail, it is not practical to provide reasonable assurance of the integrity of these voting systems by any combination of design review, inspection, testing, logical analysis, or control of the system development process.* For example, a programmer working for the machine vendor could modify the machine software to mis-record a few votes for party A as votes for party B, and this change could be triggered only during the actual election, not during testing. Many computer scientists could list dozens of other plausible ways to compromise computerized voting machines.

Most importantly, there is no reliable way to detect errors in recording votes or deliberate election rigging with these machines. Hence, *the results of any election conducted using these machines are open to question.*

Annexure 2

BUNDES-
VERFASSUNGS-
GERICHT

Federal Constitutional Court - Press office
Press release No. 19/2009 of 3 March 2009
Judgment of 3 March 2009 - 2 BvC 3/07 and 2 BvC 4/07

Use of Voting Computers in 2005 Bundestag Election Unconstitutional

The Federal Constitutional Court rendered judgment on two complaints concerning the scrutiny of an election, which were directed against the use of computer-controlled voting machines (so-called voting computers)in the 2005 Bundestag election of the 16th German Bundestag (see German press release no. 85/2008 of 25 September 2008). The Second Senate decided that the use of electronic voting machines requires that the essential steps of the voting and of the determination of the result can be examined by the citizen reliably and without any specialist knowledge of the subject. This requirement results from the principle of the public nature of elections (Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law (Grundgesetz - GG)), which prescribes that all essential steps of an election are subject to the possibility of public scrutiny unless other constitutional interests justify an exception.

Accordingly it is, admittedly, constitutionally unobjectionable that § 35 of the Federal Electoral Act (Bundeswahlgesetz - BWG) permits the use of voting machines. However, the Federal Voting Machines Ordinance

(Bundeswahlgeräteverordnung) is unconstitutional because it does not ensure that only such voting machines are permitted and used which meet the constitutional requirements of the principle of the public nature of elections. According to the decision of the Federal Constitutional Court, the computer-controlled voting machines used in the election of the 16th German Bundestag did not meet the requirements which the constitution places on the use of electronic voting machines. This, however, does not result in the dissolution of the Bundestag because for lack of any indications that voting machines malfunctioned or could have been manipulated, the protection of the continued existence of the elected parliament prevails over the electoral errors which have been ascertained. To the extent that the manner in which the German Bundestag's Committee for the Scrutiny of Elections conducted the proceedings was objected to, the complaint for the scrutiny of an election was unsuccessful.

In essence, the decision is based on the following considerations:

I. The objections to the errors of the proceedings for the scrutiny of elections which had been conducted before the German Bundestag were unsuccessful. Even though the duration of the proceedings between the lodging of the objection to the election and the German Bundestag's decision was more than a year, this is not yet a serious procedural error. The duration of the proceedings alone does not deprive the German Bundestag's decision of its foundation. Nor is the fact that the Committee for the Scrutiny of Elections refrained from conducting an oral hearing of the complainant's objection to the election, and also apart from this did not deliberate in public, a serious error which deprives the German Bundestag's decision of its foundation.

II. The principle of the public nature of elections, which results from the fundamental decisions of constitutional law in favour of democracy, the republic and the rule of law prescribes that all essential steps of an election are subject to the possibility of public scrutiny unless other constitutional interests justify an exception. Here, the examination of the

voting and of the ascertainment of the election result attains special significance.

The use of voting machines which electronically record the voters' votes and electronically ascertain the election result only meets the constitutional requirements if the essential steps of the voting and of the ascertainment of the result can be examined reliably and without any specialist knowledge of the subject. While in a conventional election with ballot papers, manipulations or acts of electoral fraud are, under the framework conditions of the applicable provisions, at any rate only possible with considerable effort and with a very high risk of detection, which has a preventive effect, programming errors in the software or deliberate electoral fraud committed by manipulating the software of electronic voting machines can be recognised only with difficulty. The very wide-reaching effect of possible errors of the voting machines or of deliberate electoral fraud make special precautions necessary in order to safeguard the principle of the public nature of elections.

The voters themselves must be able to understand without detailed knowledge of computer technology whether their votes cast are recorded in an unadulterated manner as the basis of vote counting, or at any rate as the basis of a later recount. If the election result is determined through computer-controlled processing of the votes stored in an electronic memory, it is not sufficient if merely the result of the calculation process carried out in the voting machine can be taken note of by means of a summarising printout or an electronic display.

The legislature is not prevented from using electronic voting machines in elections if the possibility of a reliable examination of correctness, which is constitutionally prescribed, is safeguarded. A complementary examination by the voter, by the electoral bodies or the general public is possible for example with electronic voting machines in which the votes are recorded in another way beside electronic storage. In the case at hand, it need not be decided whether there are other technical possibilities which make it possible for the electorate to trust in the correctness of the procedure of the ascertainment of the election result in a way that is based on

its retraceability, thus complying with the principle of the public nature of elections.

Limitations of the possibility for the citizens to examine the voting cannot be compensated by an official institution testing sample machines in the context of their engineering type licensing procedure, or the very voting machines which will be used in the elections before their being used, for their compliance with specific security requirements and for their technical integrity. Also an extensive entirety of other technical and organizational security measures alone is not suited to compensate a lack of the possibility of the essential steps of the electoral procedure being examined by the citizens. For the possibility of examining the essential steps of the election promotes justified trust in the regularity of the election only by the citizens themselves being able to reliably retrace the voting.

If computer-controlled voting machines are used, no contrary constitutional principles can be identified which could justify a far-reaching restriction on the public nature of the election, and thus on the possibility of examining the voting and the ascertainment of the result. The exclusion of ballots unwittingly being marked in an erroneous manner, of inadvertent counting errors and of erroneous interpretations of the voters' will in vote counting does not as such justify forgoing any kind of retraceability of the voting. The principle of the secrecy of the vote and the interest in a rapid clarification of the composition of the German Bundestag> are also no contrary constitutional interests which could be invoked as the basis of a far-reaching restriction on the possibility of examining the voting and the ascertainment of the result. It is not constitutionally required that the election result be available shortly after the closing of the polls. Apart from this, the past Bundestag elections have shown that also without the use of voting machines, the official provisional result can, as a general rule, be ascertained within a few hours.

III. While the authorisation to issue an ordinance, which is granted by § 35 BWG, does not meet with any overriding

constitutional reservations, the Federal Voting Machines Ordinance is unconstitutional because it infringes the principle of the public nature of elections. The Federal Voting Machines Ordinance does not contain any regulations which ensure that only such voting machines are permitted and used which comply with the constitutional requirements placed on an effective examination of the voting and a reliable verifiability of the election result. The Federal Voting Machines Ordinance does not ensure that only such voting machines are used which make it possible to reliably examine, when the vote is cast, whether the vote has been recorded in an unadulterated manner. The ordinance also does not place any concrete requirements as regards its content and procedure on a reliable later examination of the ascertainment of the result. This deficiency cannot be remedied by means of an interpretation in conformity with the constitution.

IV Also the use of the above-mentioned electronic voting machines in the election to the 16th German Bundestag infringes the public nature of the election. The voting machines did not make an effective examination of the voting possible because due to the fact that the votes were exclusively recorded electronically on a vote recording module, neither voters nor electoral boards nor citizens who were present at the polling station were able to verify the unadulterated recording of the votes cast. Also the essential steps of the ascertainment of the result could not be retraced by the public. It was not sufficient that the result of the calculation process carried out in the voting machine could be taken note of by means of a summarising printout or an electronic display.

V. The electoral errors which have been identified do not lead to a repetition of the election in the constituencies affected. The electoral error which results from the use of computer-controlled voting machines whose design was incompatible with the requirements placed on an effective possibility of examining the voting does not result in a declaration of partial invalidity of the election to the 16th German Bundestag even if it is assumed to be relevant to the allocation of seats. The interest in the protection of the

continued existence of parliament, the composition of which was determined trusting in the constitutionality of the Federal Voting Machines Ordinance, prevails over the electoral error because its possible implications on the composition of the 16th German Bundestag can be rated as marginal at most, for lack of any indications that voting machines malfunctioned or could have been manipulated, and because, also in view of the fact that the established infringement of the constitution took place when the legal situation had not been clarified yet, they do not make the continued existence of the elected parliament appear intolerable.

This press release is also available in the original German version.

Annexure 3

Newsweek

We do not trust machines; people reject electronic voting

by Evgeny Morozov | NEWSWEEK, Published May 23, 2009
From the magazine issue dated Jun 1, 2009

When Ireland embarked on an ambitious e-voting scheme in 2006 that would dispense with "stupid old pencils," as then-prime minister Bertie Ahern put it, in favor of fancy touchscreen voting machines, it seemed that the nation was embracing its technological future. Three years and •51 million later, in April, the government scrapped the entire initiative. High costs were one concern-finishing the project would take another •28 million. But what doomed the effort was a lack of trust: the electorate just didn't like that the machines would record their votes as mere electronic blips, with no tangible record.

One doesn't have to be a conspiracy theorist or a Luddite to understand the fallibility of electronic voting machines. As most PC users by now know, computers have bugs, and can be hacked. We take on this security risk in banking, shopping and e-mailing, but the ballot box must be perfectly sealed. At least that's what European voters seem to be saying. Electronic voting machines do not meet this standard.

A backlash against e-voting is brewing all over the continent. After almost two years of deliberations, Germany's Supreme Court ruled in March that e-voting was unconstitutional because the average citizen could not be expected to understand the exact steps involved in the recording and tallying of votes. Political scientist Joachim Wiesner and his son Ulrich, a physicist, filed the initial lawsuit and have been instrumental in raising public awareness of the

insecurity of electronic voting. In an interview with the German magazine Der Spiegel, the younger Wiesner said, with some justification, that the Dutch Nedap machines used in Germany are even less secure than mobile phones. The Dutch public-interest group Wij Vertrouwen Stemcomputers Niet (We Do Not Trust Voting Machines) produced a video showing how quickly the Nedap machines could be hacked without voters or election officials being aware (the answer: five minutes). After the clip was broadcast on national television in October 2006, the Netherlands banned all electronic voting machines.

Numerous electronic-voting inconsistencies in developing countries, where governments are often all too eager to manipulate votes, have only added to the controversy. After Hugo Chávez won the 2004 election in Venezuela, it came out that the government owned 28 percent of Bizta, the company that manufactured the voting machines. Similarly, the 2004 elections in India were notorious for gangs stuffing electronic ballot boxes in villages.

Why are the machines so vulnerable? Each step in the life cycle of a voting machine-from the time it is developed and installed to when the votes are recorded and the data transferred to a central repository for tallying-involves different people gaining access to the machines, often installing new software. It wouldn't be hard for, say, an election official to plant a "Trojan" program on one or many voting machines that would ensure one outcome or another, even before voters arrived at the stations. It would be just as easy to compromise the privacy of voters, identifying who voted for whom.

One way to reduce the risk of fraud is to have machines print a paper record of each vote, which voters could then deposit into a conventional ballot box. While this procedure would ensure that each vote can be verified, using paper ballots defeats the purpose of electronic voting in the first place. Using two machines produced by different manufacturers would decrease the risk of a security compromise, but wouldn't eliminate it.

A better way is to expose the software behind electronic voting machines to public scrutiny. The root problem of popular electronic machines is that the computer programs that run them are usually closely held trade secrets. (It doesn't help that the software often runs on the Microsoft Windows operating

system, which is not the world's most secure.) Having the software closely examined and tested by experts not affiliated with the company would make it easier to close technical loopholes that hackers can exploit. Experience with Web servers has shown that opening software to public scrutiny can uncover potential security breaches.

The electronic-voting industry argues that openness would hurt the competitive position of the current market leaders. A report released by the Election Technology Council, a U.S. trade association, in April says that disclosing information on known vulnerabilities might help would-be attackers more than those who would defend against such attacks. Some computer scientists have proposed that computer code be disclosed only to a limited group of certified experts. Making such disclosure mandatory for all electronic voting machines would be a good first step for the Obama administration, consistent with his talk about openness in government.

He'd better hurry, though, before a wave of populism kills electronic voting. State and local governments across the United States, much like European governments, are getting increasingly impatient with e-voting. Riverside County in California is considering asking voters to choose between e-voting and paper ballots in a referendum. Voters would be justified in dispensing with e-voting altogether. At the moment, there's very little to like about it.

Find this article at http://www.newsweek.com/id/199102

Annexure 4

The New York Times

Editorial

How to Trust Electronic Voting

Published: June 21, 2009

Electronic voting machines that do not produce a paper record of every vote cast cannot be trusted. In 2008, more than one-third of the states, including New Jersey and Texas, still did not require all votes to be recorded on paper. Representative Rush Holt has introduced a good bill that would ban paperless electronic voting in all federal elections. Congress should pass it while there is still time to get ready for 2010.

In paperless electronic voting, voters mark their choices, and when the votes have all been cast, the machine spits out the results. There is no way to be sure that a glitch or intentional vote theft - by malicious software or computer hacking - did not change the outcome. If there is a close election, there is also no way of conducting a meaningful recount.

Mr. Holt's bill would require paper ballots to be used for every vote cast in November 2010. It would help prod election officials toward the best of the currently available technologies: optical-scan voting. With optical scans, voters fill out a paper ballot that is then read by computer - much like a standardized test. The votes are counted quickly and efficiently by computer, but the paper ballot remains the official vote, which can then be recounted by hand.

The bill would also require the states to conduct random hand recounts of paper ballots in 3 percent of the precincts in federal elections, and more in very close races. These routine audits are an important check on the accuracy of the computer count.

The bill has several provisions designed to ease the transition for cash-strapped local governments. It authorizes $1 billion in financing to replace non-complying voting systems, and more money to pay for the audits. It also allows states extra time to phase out A.T.M.-style machines, in which voters make their choices on a computer screen and the machine produces a paper record - like a receipt - of the vote.

Such machines are more reliable than paperless voting. But they are still not ideal, since voters do not always check the paper record to be sure it is accurate. By 2014, machines that produce paper trails would have to be replaced by ones in which voters directly record their votes on paper - the best system of all.

The House leadership should make passing Mr. Holt's bill a priority. Few issues matter as much as ensuring that election results can be trusted.

Annexure 5

The New York Times

The Good News (Really) About Voting Machines

by Adam Cohen, The New York Times
January 10th, 2007

I. The Problem With Electronic Voting Machines

Critics of paperless electronic voting have long warned that the results cannot be trusted because it is impossible to know what goes on in the "black box," their word for the internal workings of a computerized voting machine.

The totals that the machine reports when the polls close may not reflect the choices that the voters actually made.

In the darkest scenario, the machine's manufacturer could build a computer code into it that was written to add votes to one party's candidates and take them away from another. In the summer of 2003, these fears were underscored when it was reported that the chief executive of Diebold, one of the biggest voting machine makers, had written a fund-raising letter for President Bush's campaign in which he said he was committed to delivering Ohio's electoral votes for the president - while his machines counted many of the votes in Ohio.

But the machines' manufacturers are hardly the only ones who could put malicious code on a voting machine. A single renegade employee could write vote-stealing code, or put a "patch" on the software that accomplished the same thing. Many electronic voting machines also have wireless capacity, so the results on them are vulnerable to being changed by remote technology.

There have been a number of alarming reports about how

easy it would be to hack an electronic voting machine.

Prof. Edward Felten, a computer science professor at Princeton, conducted a study recently that found that it would not be at all difficult to hack into a Diebold machine that is the most commonly used electronic voting machine in the country.

Professor Felten's two main findings were:

(1) Malicious software on a voting machine can "steal votes with little if any risk of detection." It can also "modify all of the records, audit logs and counters kept by the voting machine, so that even careful forensic examination of these records will find nothing amiss."

(2) "Anyone who has physical access to a voting machine, or to a memory card that will later be inserted into a machine, can install" malicious software in as little as one minute.

Prof. Aviel D. Rubin of Johns Hopkins University reached much the same conclusion. In a classroom exercise in 2004, he created a malicious code that was able to change the outcome of an election and then disappear without a trace.

These scenarios of intentional vote theft are the most alarming, but there is a lot that can go wrong simply by accident or with poor handling of the machines.

Voters using electronic machines have often reported that when they tried to cast a ballot, the machine "flipped" their votes from the candidate they selected to an opponent. In last November's elections, reports of "vote flipping" were widespread, and in some cases they were confirmed by election officials. In Broward County, Fla., a spokeswoman for the Board of Elections told The Miami Herald that it is not uncommon for their electronic machines to get out of sync when they are used heavily, and to register votes incorrectly. When voters call the glitches to poll workers' attention, she said, the machines can be recalibrated on the spot.

November's election brought reports of other problems with electronic voting last November, ranging from software glitches that caused votes to be counted twice to a faulty memory cartridge that caused votes to be added to races in which they

were not cast. VotersUnite.org kept a log of problems reported in the media.

II. The Solution

There is a clear answer to the problems with electronic voting: a voter-verified paper trail. That is, every time a voter casts a ballot electronically, he or she should receive a paper record that can be reviewed for accuracy. Those records should remain with the voting machine and become the official record of the vote - so if there is a conflict between the tally on the machine and the totals obtained by adding up the paper ballots, the paper-ballot tallies are the ones that are used to decide the election.

The reason is clear: as Professors Felten and Rubin and many others have shown, the results produced by electronic voting machines themselves cannot be trusted.

The National Institute for Standards and Technology , a federal agency that promotes the use of appropriate technological standards, issued a draft report (PDF) last month that explained in technical terms why paperless electronic voting systems cannot be trusted. To be credible, NIST found, a voting system must be "software independent" - that is, there must be a check on the accuracy of the system that is independent of the software in the system. The most obvious way to do that, according to NIST, is with a voter-verified paper trail.

To ensure that the vote totals are correct, after every election there should be a mandatory audit of a fixed percentage of randomly chosen machines. The paper ballots should be tabulated and compared with the votes recorded by computer, to ensure that there is no discrepancy. In New York, the law requires a manual audit of 3 percent of the paper trails from randomly chosen machines.

III. The Electronic Voting Reform Movement

The movement to reform electronic voting has been an impressive combination of leading experts and ordinary citizens.

David L. Dill, a professor of computer science at Stanford

University, has been a pioneer. Professor Dill began publicly questioning electronic voting in January 2003, and in June of that year he launched the Web site VerifiedVoting.org. VerifiedVoting.org has since become an important voice demanding that electronic voting machines produce paper trails.

Other computer scientists like Professor Rubin and the tireless Rebecca Mercuri have, like Professor Dill, used their deep knowledge of voting technology to explain the machines' security vulnerabilities to the general public.

Major national organizations, ranging from Common Cause and the American Civil Liberties Union to MoveOn.org, have played an important role in mobilizing their members and attracting attention to the issue. The national League of Women Voters, which was regrettably slow to recognize the importance of voter-verified paper trails, has recently become a strong supporter.

The most remarkable part of the movement, though, has been the grass-roots organizations that have sprung up around the country to demand better voting technology. One of the most effective of these has been New Yorkers for Verified Voting. The verified voting cause has also benefited from the energetic efforts of a few extremely dedicated activists who have made it a personal mission, people like Bev Harris of BlackBoxVoting.org, whose hard-driving style has won her both fans and critics, and Teresa Hommel of Wheresthepaper.org.

There are some powerful forces lined up on the other side. The leading opponents of paper trails have been, interestingly enough, state and local election officials and voting machine manufacturers. It is no great mystery why. Paper trails are a serious form of accountability in an area where there has been little of it. If the tallies on the paper trails do not match the totals on the machines, election officials and machine companies have to answer a lot of hard questions. Both groups would prefer to be able to certify whatever numbers show up on the machines without fear of contradiction.

Wherever paper trails have been proposed - in state legislatures, in administrative bodies - election officials have been one of the most outspoken groups to oppose them. As long

as election officials controlled the process with little input from the public, they could make decisions like these.

But since the meltdown in the 2000 presidential election, the American public has become much more aware of and concerned about the election system. Increasingly, the public's views on voting machines are prevailing, even over the opposition of election officials.

Annexure 6

The Washington Post

A Single Person Could Swing an Election

Electronic Systems' Weaknesses May Be Countered With Audits, Report Suggests

by Zachary A. Goldfarb, Wednesday, June 28, 2006; Page A07

To determine what it would take to hack a U.S. election, a team of cybersecurity experts turned to a fictional battleground state called Pennasota and a fictional gubernatorial race between Tom Jefferson and Johnny Adams. It's the year 2007, and the state uses electronic voting machines.

A Calvert County elections official demonstrates how an electronic voting machine works. (By Mark Gail — The Washington Post) WHO'S BLOGGING?

Jefferson was forecast to win the race by about 80,000 votes, or 2.3 percent of the vote. Adams's conspirators thought, "How easily can we manipulate the election results?"

The experts thought about all the ways to do it. And they concluded in a report issued yesterday that it would take only one person, with a sophisticated technical knowledge and timely access to the software that runs the voting machines, to change the outcome. The report, which was unveiled at a Capitol Hill news conference by New York University's Brennan Center for Justice and billed as the most authoritative to date, tackles some of the most contentious questions about the security of electronic voting.

The report concluded that the three major electronic voting systems in use have significant security and reliability

vulnerabilities. But it added that most of these vulnerabilities can be overcome by auditing printed voting records to spot irregularities. And while 26 states require paper records of votes, fewer than half of those require regular audits. "With electronic voting systems, there are certain attacks that can reach enough voting machines . . . that you could affect the outcome of the statewide election," said Lawrence D. Norden, associate counsel of the Brennan Center.

With billions of dollars of support from the federal government, states have replaced outdated voting machines in recent years with optical scan ballot and touch-screen machines. Activists, including prominent computer scientists, have complained for years that these machines are not secure against tampering. But electronic voting machines are also much easier to use for disabled people and those who do not speak English.

Voting machine vendors have dismissed many of the concerns, saying they are theoretical and do not reflect the real-life experience of running elections, such as how machines are kept in a secure environment. "It just isn't the piece of equipment," said David Bear, a spokesman for Diebold Election Systems, one of the country's largest vendors. "It's all the elements of an election environment that make for a secure election."

"This report is based on speculation rather than an examination of the record. To date, voting systems have not been successfully attacked in a live election," said Bob Cohen, a spokesman for the Election Technology Council, a voting machine vendors' trade group. "The purported vulnerabilities presented in this study, while interesting in theory, would be extremely difficult to exploit."

At yesterday's news conference, the push for more secure electronic voting machines, which has been popular largely on the left side of the political spectrum since the contested outcome of the 2000 presidential election in Florida, picked up some high-profile support from the other side.

Republican Reps. Tom Cole (Okla.) and Thomas M. Davis III (Va.), chairman of the House Government Reform Committee, joined Rep. Rush D. Holt (D-N.J.) in calling for a law that would set strict requirements for electronic voting machines. Howard Schmidt, former chief of security at Microsoft and President Bush's former cybersecurity adviser, also endorsed the Brennan report. "It's not a question of 'if,' it's a question of 'when,' " Davis said of an attempt to manipulate election results.

Annexure 7

Election Petition No. 5/2009 filed by Congress Candidate Alok Jena in Orissa High Court (Extracts)

***

6. That the Election Petitioner here-in-below pleads/gives Concise Statement of material facts indicating the tampering / manipulation done with respect to free / fair/ genuine recording of votes through E.V.M. by the agency entrusted to conduct free & fair Election, in order to further the prospect of winning of B.J.D. Candidates. and to ensure defeat of Election Petitioner so far as it relates to 112- BHUBANESWAR (central) Assembly Constituency :-

6- A. That, Sri Pyarimohan Mohapatra I.A.S.(Retd), who is now seating "RAJYASABHA" member of B.J.D. was in exclusive charge of managing all affairs relating to 2009 Election on behalf of Biju Janta Dal. Shri Mohapatra had served as C.E.O. of the state of Orissa for a considerable period. Most of the officers who were entrusted with the duty of conducting Election for the state were in the past working at some stage or other under Shri Mohapatra.

During the 2009 Election, Smt. Alaka Panda, was and she is still the C.E.O. of the State of Orissa. She is one of the known Honest Officer of the state. In order to frustrate her grip & control over managing the affairs of election and conducting free & fair election, a band of tainted officers having known incriminating track record were brought to manage & conduct the 2009 election. The names of these tainted officers and their incriminating track records shall be produced at the time of trial.

These tainted officers in order to save their skin from the rigors of anticipated departmental/vigilance enquiries, and to secure their future in service were eager to show and owe

more alliance to Shri.Pyarimohan Mohapatra, than to their duties and responsibilities which they are ordinarily supposed to show an owe in accordance to the respective posts they were holding under the Administrative hierarchy.

These tainted officers instead of conducting free & fair election have done anything and every thing, while they were in charge of conducting election during-2009 poll to further the prospect of winning of B.J.D. candidates & to ensure defeat of the Election Petitioner at the behest of Shri Pyarimohan Mohapatra, which would be evident from concise statements or material facts given in the following Paragraphs.

6-B. That in the state of Orissa, there are 147Assembly Constituencies. During 2009Election, polling was conducted in two phases. In the first phase of Election polling was conducted in 70 Assembly Constituencies, on16.04.2009. Out of the aforesaid 70 Assembly Constituencies of the first phase 12 Assembly Constituencies were of Ganjam District and rest 58 Assembly Constituencies were of other districts. In these 58 Assembly Constituencies in which election was held on16.04.2009, the B.J.D. candidates have won only in 28 seats.

The second phase of election was held on 23.04.2009. Polling with respect to 70 Assembly Constituencies were conducted on this date. Thus, the second phase 77 Assembly Constituencies and 12 assembly Constituencies of Ganjam district in which polling was held on16.04.2009, which together 89 Assembly Constituencies, the B.J.D. candidates have won in 81 Assembly Constituencies.

The difference in ratio of success of the BJD candidates it self is an indicator that in the aforesaid 89 Assembly Constituencies the ruling party, B.J.D. has won by mere manipulation / tampering of the Electronic Voting Machines (EVM). The results of election in these 89 assembly Constituencies are not out come of free & fair election but an outcome of tampering / manipulation of EVMS. The election petitioner herein after has given/ pleaded concise statement of material facts as to how manipulation / tampering in the EVM has been caused in the above 89 assembly Constituencies including the election petitioner's Constituency i.e. 1 12 Bhubaneswar (central) assembly Constituency.

6-C. That the election petitioner in this paragraph gives/ pleads a concise statement of material fact indicating how stage

by stage systematically manipulation/tampering of EVM has been perpetrated. In Orissa there are 147 assembly Constituencies, the total number of booths in these 147 assembly Constituencies are 31,617. During 2009 poll, simultaneous election for assemblies as well as for parliament was being conducted. Therefore the minimum requirement of EVM's to cater to the above need was 63,234.

In addition to the above keeping more or less 25% of extra margin in requirement of additional EVM's, the state election agency appears to have decided to procure 80,000 EVM's to conduct the poll.

According to law and instructions of the election commission, these EVM's were to be procured from recognized / authorized manufacturer/supplier. In express violation of the above rule and instructions of the election commission, the agency in charge of conducting the state election for the reasons best known to them procured 80,000 EVM's through Idcol Software limited. Which is a Government of Orissa Undertaking and a group of hand picked tainted officers were kept in its controlling and managing positions at the behest of Sri Pyarimohan Mohapatra, during the relevant period in order to complete the process for EVM procurement.

The genuinety of these EVMS were not demonstrated to the political parties and Candidates. The trustworthiness of these machines were never tested nor demonstrated nor it was ever demonstrated that appropriate safety measures have been installed in these machines as directed by the Hon'ble Supreme Court and Election Commission of India to ensure these machines to be tamper proof and trust worthy.

6-D. That, these EVM's were procured in two phases. In first phase 74,000 EVM's were procured but the same were not brought to office of the chief electoral officer at Bhubaneswar nor to a place nearer to the office of the Chief Electoral Officer at Bhubaneswar. On the contrary it was directed to be stocked/ stored in the abandoned godown of Konark Jute mill at Dhanmandal. In second phase 6000 EVM's were stocked and stored in unit-ix, High School, Bhubaneswar.

A specially designed / programmed electronic device is attached/ installed to majority of such 80,000 EVM's which were used in most of the booths of these above 89 Assembly Constituency, in order to ensure systematized transfer of votes

recorded by the voters in the balloting units to be stored in favour of BJD candidates In the respective control units in a ratio of 70 to 80 percent of the total votes recorded in each balloting units. These statement will be apparently evident on a bare comparison of votes recorded constituency wise in all the EVM's of above 89 Assembly Constituency including 112-Bhubaneswar (Central) Assembly Constituency.

6-E. That, the next stage of manipulation/tampering was designed to be effected by change of EVMS without notice to any body which would be clearly evident from the very fact that the first notice in this respect was circulated on 15.04.2009 specifying the identification number and machine number of each balloting unit and identification number and machine number of each controlling unit and indicating in the notice as to at which polling station the same shall be put to operation together with a list of reserved balloting unit as well as controlling units with its identification number and machine number, so far it relates to 112-Bhubaneswar(Central) Assembly Constituency.

This notice / circular was not communicated to the election petitioner nor the test functioning of the EVM's were demonstrated to the contesting candidates.

On 20.04.09 under notification number 1058 reference of change /substitution was given with respect to booth No-1, booth No-88 both control unit and balloting unit and reference of one set of control unit and balloting unit was mentioned to be kept as reserve units. No intimation of this was given to the election petitioner. The election petitioner only come to know about this change on inquiry after publication of the shocking result of counting held on 16.5.09.

The petitioner further came to know after counting that a change has been done before or during poll with respect to the EVMS deployed in booth No148,152,86 and 72. A notice of such change was said to have been published on 29.04.09 under notification no-1159. However this notification is subsequent to the date of polling. The change of EVMS in the above four booths were done without the knowledge of the election petitioner and without any intimation to him, and / or his election agent and / or polling agents.

Curiously enough to the utter surprise of the petitioner on

verification it is found that, in 39 booths/ polling stations balloting units and controlling units as mentioned in the aforesaid notifications dt.15,04.2009 & 20.04.2009 were not used but different EVM units were used having totally different identification number and machine numbers. The number of these booths are booth no. 1, 4, 5, 7, 11, 16, 24, 55, 57, 58, 66, 72, 84, 86, 88, 91, 95, 96, 98, 102, 104, 105, 106, 108, 112, 115, 116, 117, 122, 127, 129, 134, 139, 148, 149, 150, 152, 159 & 162. The total votes shown to have been recorded in the respective EVM's in the above 39 booths is 19, 464 out of which in favour of first respondent 12106 vote have been recorded. This being the position it is apparent that the recording of votes in the above booths are not trustworthy and/ or legally acceptable. Therefore the result declared on 16.05.2009 declaring the respondent no-1to have secured more votes i.e.46417 is not the out come of true & genuine figure but on the contrary is out come of tampering / manipulation and change of EVM's. In the above 39 booths mock poll was also not demonstrated.

That in addition to the above booth numbers, the election petitioner here in below gives reference of 31booths, such as booth no. 2, 3, 15, 22, 23, 25, 37, 38, 46, 47, 49, 50, 62, 71, 85, 87, 89, 94, 109,111, 118, 120, 121, 132, 140, 141, 151, 153, 155, 156, 161. In these 31 booths there has been rampant manipulation and votes in these booths have been recorded by rigging. This fact will be evident from examination of Register of voters maintained in form 17A. The written complaint of respective polling agent of the election petitioner in the above booths were not accepted by the presiding officers. In all these booths no mock poll was demonstrated. The total number of votes shown to have been recorded in the EVM's in the above 31 booth is 17385 and the vote recorded in the favour of the first Respondent is 11244. In respect of the 92 booths total votes recorded in favour of first respondent is 23050. If verification is made it will be seen that before commencement of polling in each polling station 100 to 150 votes have been illegally recorded by the polling personals at the behest of Sri Pyarimohan Mohapatra in all the above162 booths which in aggregate comes to 20000 votes. Thus the total number of illegal recording of votes in the EVM's, in above three ways comes to 43350 votes (12106+11244+20000). The votes so

illegally recorded being void votes are to be excluded. Thus the election petitioner has received more valid votes than the first respondent.

6 (F) That as a matter of fact voting through EVM is not trustworthy for the following reasons :

a) It has no tangible record.

b) The voter has no opportunity to see that the vote recorded by him has been in fact recorded in favour of the candidate of his won choice.

c) Before the actual voting starts & votes are recorded by the voters and the data is transferred to a central repository for tallying, it involves different people gaining excess to the machine installing a parallel programme under another pass word in the voting machine that would, before voters arrived at the polling stations can ensure a predetermined poll outcome.

***

Annexure 8

Civil writ petition No. 11879/ 2009 filed by Subramanian Swamy in Delhi High Court (Extracts)

***

5 (c) International standards an election has to meet, to be credibly considered free and fair, comprehend:

(i) individuals have to be accurately identified as eligible voters who have not already voted;

(ii) Voters are allowed only one anonymous ballot each, which they can mark in privacy;

(iii) The ballot box is secure, observed and, during the election, only able to have votes added to it by voters: votes cannot be removed;

(iv) when the election ends, the ballot box is opened and counted in the presence of observers from all competing parties. The counting process cannot reveal how individual voters cast their ballots;

(v) if the results are in doubt, the ballots can be checked and counted again by different people;

(vi) as far as the individual voter is concerned ,he must be assured that the candidate he casts his vote for, actually gets that vote.

Over the last few centuries, the system of paper ballots has been developed which can meet all six requirements. But, it is submitted, the present system of EVMs as utilized in the last few general elections in India,(though admittedly it gives results very fast and dispenses with the labour of hand counting) do not meet requirements (v) and (vi).

(d) Particularly in the last two decades, electronic voting was introduced in many countries worldwide; but after utilizing them for a short while serious doubts were raised about the

security, accuracy, reliability and verifiability of electronic elections. In October 2006 the Netherlands banned all EVM's. In 2009, the Republic of Ireland declared a moratorium on their use. Italy too has followed suit. In 2007, after conducting a top-to-bottom review of many of the voting systems certified for use in California, its Secretary of State strengthened the security requirements and use conditions .In particular, California now requires all EVMs, used at election time, to have paper backups. Thereafter, till today at least a further 27 states of the US have followed suit.

6. (a) The reason for this suspicion and rejection lies in the nature of EVMs. : doubts have been rightly raised that their software is liable to be misutilized by "Trojan Horses": a Trojan is a malicious code, sneaked in under the guise of another program, that sits silently in the original software, which goes undetected and can be activated through a key code and which is known only to the developer who inserts it .At the appropriate time, the Trojan then executes its malicious code after which quite often it will self destroy.

(b) Thus by introducing in the EVM a Trojan, whether before or after polling, the machine is programmed to alter the voter's indicated choice, in order to favour some other candidate. It is to state the obvious to state that it is the duty of the Election Commission to ensure that no EVM is used that could contain such a Trojan. Thus it has to ensure that its EVM's are not only incapable of harbouring any Trojan known to exist at the time the EVM is designed and manufactured; but also it must be incapable of harboring a Trojan which (by virtue of the continually developing phenomena of new techniques of hacking and the development of new Trojans) can ever be developed even after the EVM has been manufactured.

(c) This is not a flimsy demand. Just this month at the 2009 Electronic Voting Technology Workshop, computer scientists have demonstrated how criminals could hack an EVM and "steal" votes using a malicious programming approach that had not been invented when the voting machine was designed. Appended hereto as Annexure P-2 Colly is a news item that appeared in the Times of India, Delhi edition on 12.8.2009. and of the blog on which it is based.

(d) Hence the reason why all responsible authorites in charge of conducting elections are insisting on a paper backup.

7. The question arises as to what this "paper backup" comprehends.

(a) As suggested and developed by many experts, this paper backup, or "paper trail" procedure is to supplement the procedure of voting, as follows:

"Once approved, the voter views the ballot and makes the desired selections .....If the voter confirms that the choices displayed are correct ,the machine records the vote on some storage medium such as a CD-ROM or flash memory and overwrites the smart card with random numbers to prevent its reuse .....The voting machine then prints out a human readable ballot ,which is confirmed by the voter, who then deposits it in the ballot box , which poll workers are monitoring. If the election is later disputed, officials can optically scan these paper ballots or hand-count them."(See May 2009 issue of the IEEE Computer Society, pages 23 to 29, Article by Nathanael Paul and Andrew S. Tannenbaum:"Trustworthy Voting: From Machine to System" appended hereto as Annexure P-3)).

(b) A further safeguard to the above procedure, has also been developed, viz. that at the time of issuing the stamped paper ballot, the EVM also issues to the voter to take home, a print out receipt indicating exactly how he voted. The reason why this receipt is a good precaution, is as follows: presently, if an election is challenged on the ground that some particular identified voter's vote or the vote of a group of voters has been suppressed/not been correctly assigned, the accepted procedure is for such voter/voters to submit an affidavit stating as to how he/they had voted; and then it is for the Court to decide the credibility of such depositions. Under the new procedure, no affidavit is necessary: all that the voter has to do, is to submit the printout receipt the EVM had issued to him.

(c) It is to be emphasized that printing such a paper receipt and handing it over to the voter, does not in any way violate the right of that voter to secrecy of that voter's vote: only that voter has the receipt, and it is up to him to keep it hidden or publicise it, as he chooses.

(d) To summarise, when a voter votes, the suggested EVM with the paper trail, does three things:

1. It records the vote electronically;

2. It prints a paper vote that the voter can read, and verify before depositing in a separate ballot box;

3. It prints a receipt for the voter that he can take home as proof whom he voted for.

Thus in the event that any group of voters look at their receipts and detect an anomaly with the electronic result, they have due cause to require an election audit, and the ballot box provides the audit trail that can actually be counted.

(e) With such an indicated paper trail, in order to rig this election, the intending fraudster would need to identically rig:

(i) the electronic counter;

(ii) the paper ballot boxes;

(iii) the distributed paper receipts.

Which is virtually impossible.

(f) In a further modification of the EVM , one can link the EVM with the projected UID(Universal Identification) and have it check the voters' fingerprints-biometric details---, before allowing them to vote, this will eliminate bogus voters as well.

(g) All the above modifications are both easily and cheaply available.

8. Nor, it is submitted, is such a paper trail arcane or unusual or difficult. In at least two every day transactions, Indians have been using it:

(a) In all railway booking,(whether obtained online or at a railway booking office), a ticket/printout is issued. This is precisely the "paper trail" which assures the purchaser that his ticket has indeed been booked. It is difficult to visualize a traveler who would be satisfied, after booking his ticket, to get no paper verification at all, but has simply to rely on what is (invisible to him) recorded in the railway computers.

(b) When a bank's customer draws money from an ATM machine, he gets a printed receipt which itemizes the present details of his bank account including the present withdrawal. He can also go to the bank and get a printed confirmation of his account. It is impossible to visualize a customer who would put his money in a bank where he gets neither a receipt for his withdrawal/deposit, nor a printed statement of his account.

13 (c) The latest General Elections to the Lok Sabha, held in April-May 2009,were conducted wholly with the use of EVMs. Around 13,60,000 such machines were used in 828,000 polling booths. Thereafter Writ Petitions voicing concern over the credibility of EVM results have been filed in various High

Courts. An Andhra Pradesh based NGO, Election Watch, filed in the Supreme Court of India W.P.(C) No.292/2009, a P.I.L. which itemized in detail the manner in which such EVMs can be manipulated. Its prayers were:

"The petitioners therefore, pray that in the facts and circumstances of the present case this Hon'ble Court may be pleased to issue a writ of Mandamus / certiorari or a writ / direction of like nature to:

(i) Direct the Respondents to provide such mechanism which is free from any manipulation/tampering so that free and fair elections in the parliamentary democracy are ensured and that the votes cast by the citizens as their right of free expression under Article 19(1)(a) of the Constitution are reflected correctly in such mechanism, whether EVM or ballots or any other device.

(ii) Direct appointment of an Independent Expert Committee to study in details all the aspects / objections concerning the present EVMs and submission of the said report before this Hon'ble court for passing appropriate orders.

(iii) Pass such other order/orders as this Hon'ble Court may deem fit and proper in the circumstance of the case. "

On 27.7.2009,the Hon'ble Supreme Court disposed of W.P.(C) No.292 of 2009, with a direction to approach the Election Commission with its information. This the Election Watch has done, with what result is set out hereinbelow.

14.(a) Thus, after studying all the data in regard to the results of the 2009 Lok Sabha General Elections, the Petitioner sent a legal notice, dated 29.5.2009,appended hereto as Annexure P-5 to the Election Commission demanding that a paper trail ,as indicated be put in place.

(b) On 27.7.2009, more than two months later, the Petitioner received the Election Commission's reply dated 27.7.2009, Annexure P-6 ,to his aforesaid letter of demand. In brief, the Election Commission reiterated its stand that its EVMs were tamper proof and it had taken all precautions to ensure that they never fall into the hands of any unauthorized persons. As to the Petitioner's specific demand that it set up a paper trail, the Election Commission simply declined to do so , stating:

"As regards your suggestion for introduction of the paper trail in the ECI-EVMs, it is stated that when vote is recorded,

light glows against the name and symbol of the candidate, which is electronic equivalent of a paper output. The Commission, therefore, does not consider that a parallel maintenance of paper trail is necessary since the person who is bent on doubting would ever doubt the paper output by the machines. "

15(a) By then, the Hon'ble Supreme Court's Order disposing of Election Watch's Writ Petition was issued; and the Election Commission had invited Election Watch to demonstrate before it how its EVMs could be tampered with. Before he could take any action in regard to his demand for a paper trail, Election watch invited the Petitioner to accompany them and obtained Election Commission's leave to be present at their demonstration.

(b) Two hearings of the Election Watch have been held before the Election Commission. At the first hearing, on 17.8.2009, the Election Commission failed to present its EVMs and the manufacturers' engineers who serviced them, so the matter had to be adjourned.

(c) Before the next hearing, on or around 1.9.2009, Election Watch was served with a legal notice from ECIL, threatening them with a suit for defamation, for ststing that their EVMs could be tampered with, and demanding an apology in writing.

(d) Accordingly at the second hearing, Election Watch requested the Election Commission representative there to assure them that they would be ensured/indemnified against such suit for defamation, by the manufacturers of the Election Commission's EVMs. This assurance, the Election Commission representative stated that he was not authorised to give, but the Commission requested the ECIL to "consider" withdrawing the said Notice; The ECIL however remained adamant. Despite this attempt at intimidation, the Election Watch decided to go ahead with the demonstration after consultations with this Petitioner. It was agreed that as a first stage, only ECIL's employees would open the actual machines and then Election Watch experts would handle the parts and make notes thereon.

(e) However, when the Election Watch experts began to make notes about the parts, the manufacturers' engineers objected and demanded that the notes be confiscated. The Election Commission representative stated that he was not authorized to let the inspection go on under these circumstances. The demonstration was therefore adjourned by

the Election Commission so that orders thereon from the Election Commissioners could be obtained.

(f) So far, neither the Petitioner nor Election Watch has been apprised of anything further . Meanwhile ECIL's legal notice has not been withdrawn. Accordingly it is apprehended that further tests on the EVMs maybe delayed indefinitely until the legal liability issue are decided. Meanwhile, election after election is being scheduled and carried out without any safeguard in place.

16. Meanwhile on the same date, 3.9.2009, the Petitioner, who had merely asked for videos of the demonstrations, was e-mailed a letter from the Election Commission challenging him to prove that the EVMs could be tampered with. Since at no stage had the Petitioner averred that these EVMs were tampered with (at this stage, he is only demanding a paper trail to be put in place as per international consensus for building voter confidence) at the hearing ,the Petitioner demanded that the letter be withdrawn. The Petitioner also sent a letter dated 3.9.2009, Annexure P-7, heretoreiterating his stand.

***

17. Accordingly, it has become necessary to challenge the Respondent's letter dated 27.7.2009, to the Petitioner, refusing to accede to the Petitioner's demand for a paper trail. Being aggrieved thereby, the Petitioner is approaching this Hon'ble Court under Article 226 of the Constitution of India ,for relief on the following among other grounds. These grounds are taken in the alternate and without prejudice to one another.

Grounds:

A. It is the duty-indeed the raison d'etre--- of the Election Commission to ensure free and fair elections. International standards which an election has to meet, to be considered free and fair, comprehend the following:

(i) individuals have to be accurately identified as eligible voters who have not already voted;

(ii) voters are allowed only one anonymous ballot each, which they can mark in privacy;

(iii) the ballot box is secure, observed and, during the election, only able to have votes added to it by voters: votes cannot be removed;

(iv) when the election ends, the ballot box is opened and

counted in the presence of observers from all competing parties. The counting process cannot reveal how individual voters cast their ballots;

(v) if the results are in doubt, the ballots can be checked and counted again by different people;

(vi) as far as the individual voter is concerned ,he must be assured that the candidate he casts his vote for, actually gets that vote.

With the present EVM's used by the Election Commission, if anyone doubts the election result and demands a recount , all that can be done is that the EVM can go through its stored electronic data once more: it cannot check whether someone's vote has been properly recorded and stored because it has just the one record.. So all that happens is that the EVM goes through the same record and gets exactly the same result i.e. a recount is not a fresh operation, but merely the same operation carried out again on the same (perhaps flawed) data. Thus the requirement of (v) and (vi) are not met.

On the other hand, with a paper ballot, a different set of officials can re-sort the vote bundles by hand and recount by hand and ,in case a person's vote has been put (whether deliberately or by accident) into the wrong candidate's bundle, this can be corrected and a fresh correct result obtained.

B. In case a voter notices an anomaly in the vote results, e.g. a group of persons who have voted in the same polling booth and who have voted for one candidate, discover on publication of the voter's tally, that their candidate was credited with less votes than they know to have been polled by his supporters, there is no relief they can get from an EVM recount. On the other hand ,if these persons all present to the Returning Officer/designated official their vote receipts ,the malfeasance becomes indubitable and evident. In such a case , there can be a fresh recount by hand of the paper ballots placed in the Ballot box; and this and only this recount can be declared as the correct tally.

C. Judging by its letter dated 27.7.2009, the Election Commission has not even understood how the paper trail works.The letter states:

"7. As regards your suggestion for introduction of the paper trail in the ECI-EVMs, it is stated that when vote is recorded, light glows against the name and symbol of the candidate,

which is electronic equivalent of a paper output. The Commission, therefore, does not consider that a parallel maintenance of paper trail is necessary since the person who is bent on doubting would ever doubt the paper output by the machines. Moreover, the ECI-EVMs have the facility of paper trail in the form of a device called the 'decoder' which when attached to the EVM can print out statements of voting data showing the order in which the voters voted and to whom (i.e. the serial number pertaining to the particular candidate in the ballot paper) they voted "(emphasis supplied)

In fact, it is precisely the voter's apprehension that the glowing light may reflect his choice, but the record inside the EVM may be quite different: he has nothing to assure him that his vote has been properly recorded inside the EVM.

On the other hand ,if when he votes he gets a paper ballot and a paper receipt with the print out of his choice, and he then checks it and assures himself that it is correct, and then he places this paper ballot himself in the ballot box and takes away the paper receipt with him, then he is sure that in case of a malfeasance,(which he can prove by displaying his paper receipt) he can demand a count of the ballot box paper ballots. He would not "ever doubt the paper output by the machine",: because he has himself read it and confirmed his vote at the time he votes.

As to the decoder, it will only tell you what the machine states is the vote cast at a particular time. But ,in case it is the voter's contention that the vote the EVM states was cast at a particular time is wrongly recorded, there is no proof in his hand to give the lie to the EVM.

D. As to the Election Commission's plea of sacredness of the secrecy of the voter's choice, it is pointed out that :

(i) admittedly the decoder has a printout facility; but this printout only repeats what is recorded in the EVM (which may or may not be the voter's actual choice);

(ii) the proposed printed receipt in the hand of the voter is totally under his control; and if he does not choose to make it public, no one can force him to. On the other hand, if suspecting malfeasance ,he takes it to the Returning Officer/ concerned authority, to prove the malfeasance, that also is his choice. In neither case is his right to secrecy of his vote violated.

(iii)the contents of the paper ballot box can be counted without in any way revealing any particular voter/locality's preference, so again there is no violation of the secrecy of a voter's/locality's vote.

(iv) if, as the Election Commissioners have averred in meetings, the problem arises because a voter who walks out of the polling booth carrying his printed receipt may be suborned by some party supporter standing outside the booth who terrorizes him into revealing what is on the receipt, and then proceeds to manhandle the voter if his vote proves to have been for some rival candidate, it is submitted that the correct solution is simply to provide better protection to this voter, so that no one can forcibly get to know how he voted. It can never be an argument that a vital safeguard like the Paper Trail, must not be followed because there are party goondas who cannot be controlled by the Government and the forces of law and order. Nor should the Election Commission encourage a practice like a voter being bound to show his receipt to prove his bonafide voting to someone who has paid him to vote in a particular fashion, and who demands the printed receipt as proof that he has carried out what he was bribed to carry out.

(v) The voter's right to be assured that his vote has actually been credited to the candidate of his choice, far outweighs the personal difficulties and hardship ,and exposure to harassment that he or someone else may suffer because some goondas force him to show his receipt.

(vi) In any event, nothing prevents a reluctant voter from destroying his paper receipt if he so wishes: the paper ballot in the ballot box is all that is required in the case a recount is demanded.

E. The best retort to the Election Commission's stand that its EVMs are infallible and the material is correctly recorded therein, and there is no need for a paper receipt for the voter, is to ask any voter the parallel question,

"Would you put your money in a bank with an ATM facility, where the machine neither gives you a receipt, nor does the bank ever give you an accounting/proof of your transaction?"

***

Around the world, most countries using stand-alone Electronic Voting Machines (EVMs) have been discarding them - as voters cannot be sure that their votes have been correctly recorded and there can be no possibility of a proper recount in case of disputes.

Germany, Holland and Ireland have gone back to paper ballots, and most states in the US now mandate a "Voter Verifiable Paper Trail" along with use of EVMs.

Though these same concerns (of the vulnerability of EVMs to external hacking and internal fraud) have been raised in India and there are legal challenges before the Courts, the Election Commission of India has been stoutly resisting any serious examination of the issue not to speak of considering possible solutions and reform.

In our system of representative democracy, elections provide the only occasion when the people directly exercise their sovereign power. Immediately thereafter, this power is ceded to the elected representatives. If this sacred power is vitiated by a voting system of dubious integrity open to insidious fraud, it is evident that our democracy is seriously endangered.

There is insufficient appreciation among the lay public of the facts and issues about this matter that vitally concerns them - largely due to the mystique concerning anything technological, and to implicit faith in a constitutional body such as the Election Commission. This book has been written with the objective of filling this information and awareness gap.

G.V.L. Narasimha Rao, 45, is a leading survey researcher, election analyst and political commentator. His columns and articles have appeared in Mint, the Times of India, the Economic Times and other newspapers. He appears regularly on television in election related shows. He became a national executive member of the BJP last year. He can be contacted at nrao@drsindia.org

Veta
Citizens for
Verifiability, Transparency
& Accountability in Elections

Rs. 295